8 port 10/100TX plus 2 port 100FX Managed Industrial Switch

HME-821 (multimode) HME-823 (singlemode)

User Manual

Rev.2.0

Oct.-2006

Notice

The manual contents are based on the table below listing software kernel version, hardware version, and firmware version. If the switch functions have any different from the manual contents description, please contact the local sales dealer for more information.

Firmware Version	V1.00
Kernel Version	V1.12
Hardware Version	----------

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Contents

Introduction

The 8 port 10/100TX plus 2 port 100FX managed industrial switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. The managed industrial switch can be easily managed through the Web GUI. Using the fiber ports can extend the connection distance that increases the network elasticity and performance. It also provides the X-Ring Redundancy function that can prevent a network connection failure.

Features

- Conforms to IEEE 802.3 10Base-T, 802.3u 100Base-TX/100BASE-FX
- 8-port 10/100TX plus 2 port 100FX ports (821 – multimode, 823 – singlemode)
- RJ-45 ports support auto MDI/MDI-X function
- Store-and-Forward switching architecture
- Wide-range redundant power design
- DIN rail and wall mount design
- Easy configuration setup
- 8K MAC address table
- Web management GUI
- Each port supports 4 priority queues
- Provides Fiber link ability – 2 FX ports (HME-821 multimode, HME-823 singlemode)
- IEEE 802.3x flow control support
    - Flow control with full-duplex
    - Back pressure with half-duplex
- Supports Class of Service (COS)
- Supports IGMP with Query mode for multi media applications
- Supports ingress packet filtering and egress rate limiting.
- Supports SNTP/SMTP
- Port mirroring for TX or RX or TX and RX packets.
- Alarm Relay output for system events

- Supports X-Ring redundancy function
- Power polarity reverse protection
- 1Mbits Embedded memory
- Supports Port based VLAN / 802.1 Q Tag VLAN
- Quality of Service:
  - Supports IEEE 802.1p class of service
  - Each port provides 4 priority queues
  - Port based/Tag based, IPv4 ToS, IPv4 Different Service
- Supports DHCP client
- SNMP, Web Management, RMON supported
- TFTP firmware update and system configuration restore and backup.

Package Contents

Please refer to the package content list below to verify them against the checklist.

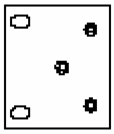
- 8 -10/100TX plus 2 -100FX (821 – multimode, 823 – singlemode) switch
- User manual
- RS-232/RJ-45 cable
- Power Terminal Block connector
- DIN-Rail mounting clip (attached on the switch)
- 2 wall mount plates and 6 screws (optional)

8 10/100TX plus 2 100FX managed industrial switch

User Manual

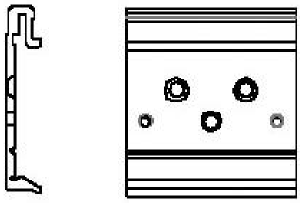
RS-232/RJ-45 connector cable

block connector



Wall Mount Plate

Screws



DIN-Rail

Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

Hardware Description

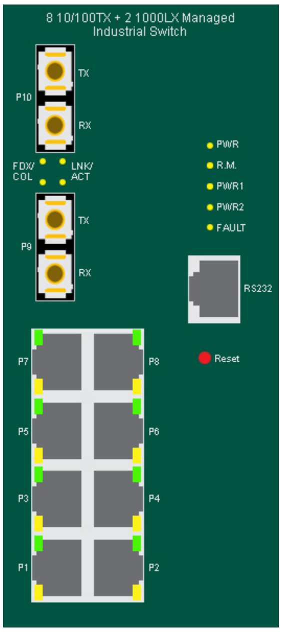
In this section, we will describe the Industrial switch’s hardware specification, ports, cabling information, and wiring installation.

Physical Dimensions

8 10/100TX plus 2 100FX managed industrial switch dimensions (W x D x H) are **72mm x 105mm x 152mm**

Front Panel

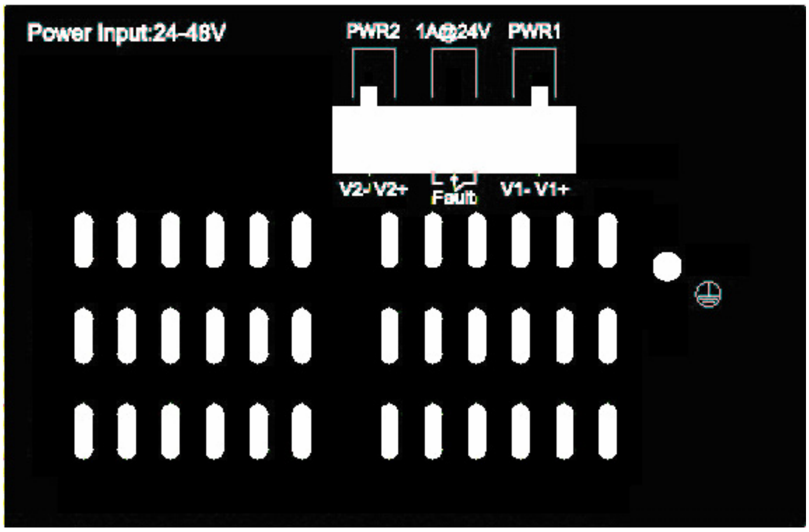
The Front Panel of the 8 -10/100TX plus 2-100FX managed industrial switch is showed as below:



Front Panel of the industrial switch

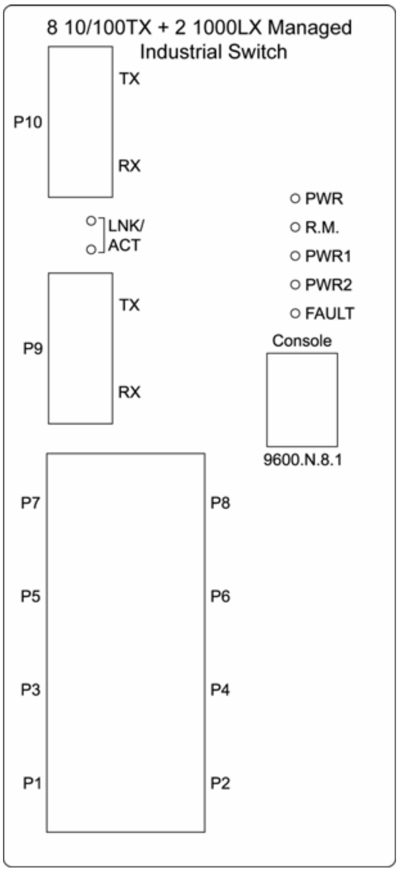
Bottom View

The bottom panel of the 8 -10/100TX plus 2 -100FX managed industrial switch has one terminal block connector within two DC power inputs and one DC IN power jack.



Bottom Panel of the industrial switch

LED Indicators



LED indicators

There are 7 diagnostic LEDs located on the front panel of the industrial switch. They provide real-time information of system and optional status. The following table provides description of the LED status and their meanings for the switch.

LED	Status	Meaning
PWR	Green	The switch unit is power on
	Off	The switch unit has no power
PWR1	Green	Power on
	Off	No power to input PWR1
PWR2	Green	Power on

	Off	No power to input PWR2
Fault	Orange	Power failure or UTP port failure or Fiber port failure
	Off	No Problems
R.M.	Green	The industrial switch is the master of X-Ring group
	Off	The industrial switch is not a ring master in X-Ring group
LNK/ACT	Green	The fiber port is linking
	Blinks	The port is transmitting or receiving packets from the TX device.
	Off	No device attached
P1 ~ P8	Orange	The port is operating in full-duplex mode.
	Blinking (Orange)	Collision of Packets occurs.
	Off	The port is in half-duplex mode or no device is attached.
	Green	A network device is detected.
	Blinking (Green)	The port is transmitting or receiving packets from the TX device.
	Off	No device attached

Ports

- **RJ-45 ports**

There are 8 x 10/100Mbps auto-sensing ports for 10Base-T or 100Base-TX device connections. The UTP ports will auto-sense for 10Base-T or 100Base-TX connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the below figures for straight through and crossover cable schematic.

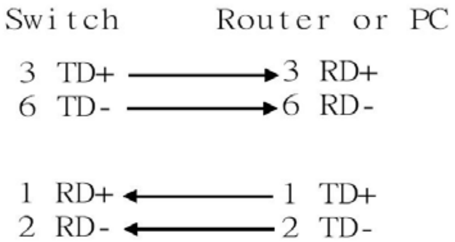
- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

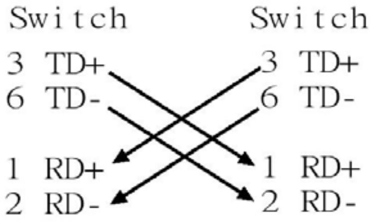
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

All ports on this industrial switch support automatic MDI/MDI-X operation, user can use straight-through cables (See figure below) for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/100BASE-TX MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)



Straight Through Cable Schematic

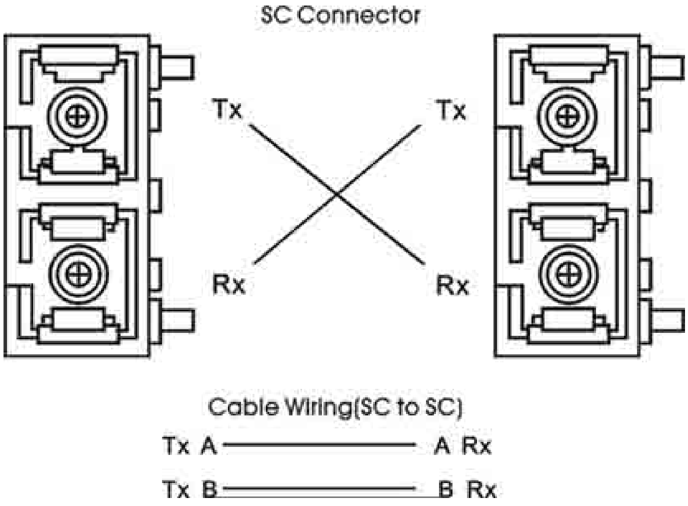


Cross Over Cable Schematic

■ Fiber Port

There are two 100Base-FX ports. The fiber port has an SC type connector for the multi mode HME-821 (2Km) or single mode HME-823 (30Km).

When a user connects the fiber port to another fiber port, please follow the figure below to connect it. A wrong connection will not allow the port to work.



ATTENTION

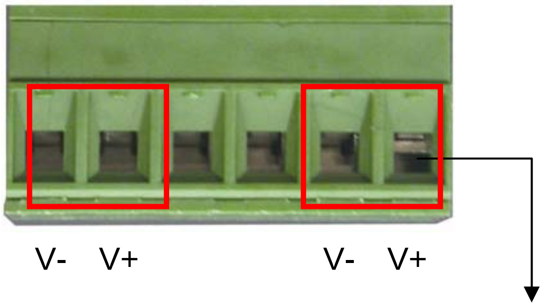
This is a Class 1 Laser/LED product. Don’t stare into the Laser/LED Beam.

Cabling

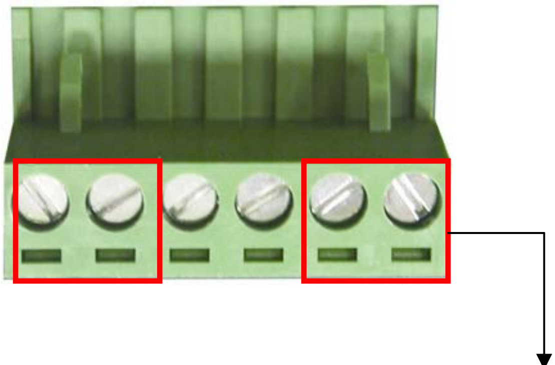
- Use four twisted-pair, Category 5 cabling for RJ-45 port connections. The cable between the converter and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Fiber segments using **single-mode** cabling must use 8/125 or 9/125 um single-mode fiber cable. The User can connect two devices up to a distance of **30 Kilometers**.
- Fiber segments using **multi-mode** cabling must use 50 or 62.5/125 um multi-mode fiber cable. The User can connect two devices up to a distance of **2 Kilometers.**

Wiring the Power Inputs

Please follow the steps below to insert the power wires.



1. Insert the positive and negative wires into the V+ and V- contacts on the terminal block connector.

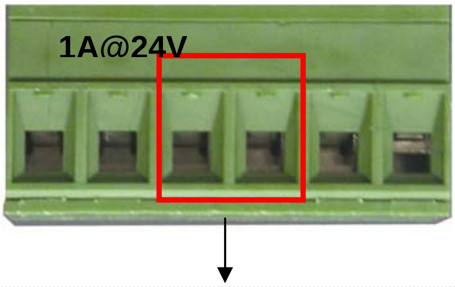


2. Tighten the wire-clamp screws to prevent the DC wires from loosening.

[NOTE] The wire gauge of the terminal block is from 12~ 24 AWG.

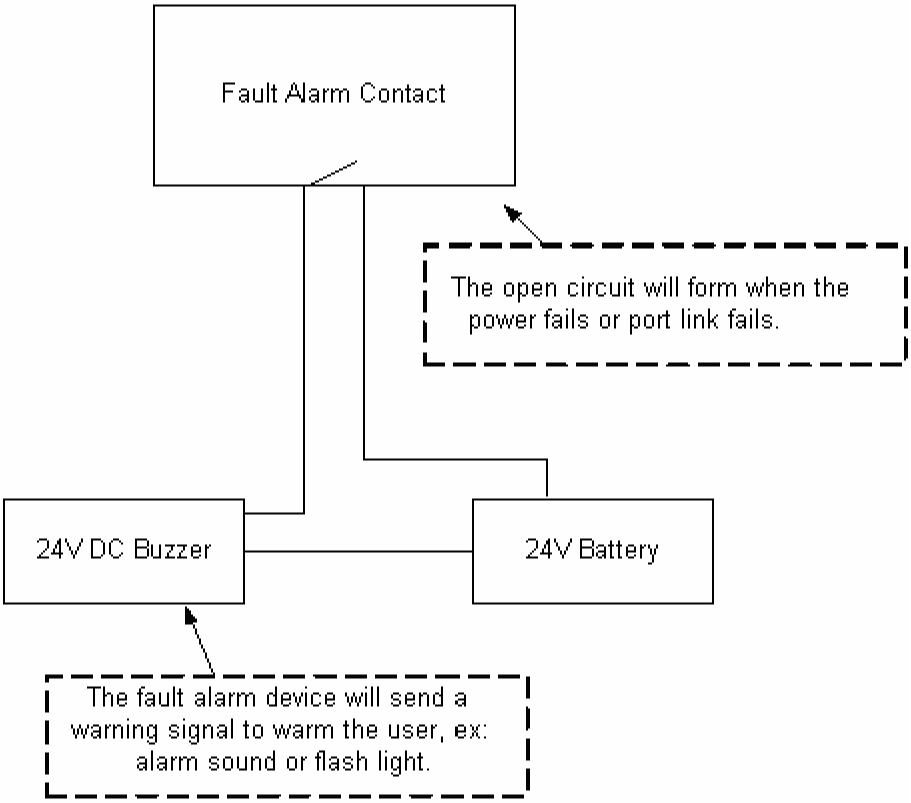
Wiring the Fault Alarm Contact

The fault alarm contact is in the middle of terminal block connector as the picture shows. If used, it will detect the fault status - power failure of PWR1 or PWR2 or port link failure and will close a normally open contact. An application example for the fault alarm contact is below: Capacity of the N.O. contact is 1.0 Amp @ 24VDC.



Insert the wires into the fault alarm contact

[NOTE] The wire gauge of the terminal block is from 12~ 24 AWG.



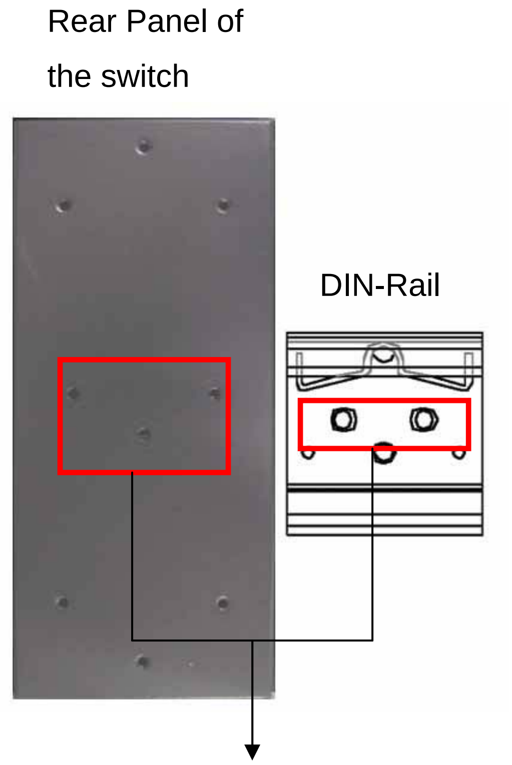
The open circuit will form when the power fails or port link fails.

The fault alarm device will send a warning signal to warm the user, ex: alarm sound or flash light.

Mounting Installation

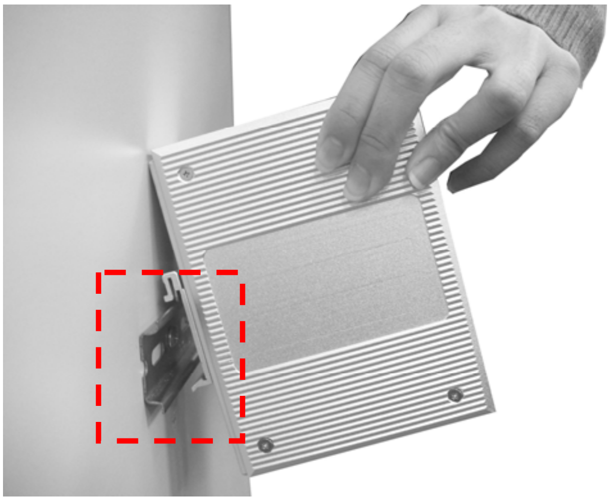
DIN-Rail Mounting

The DIN-Rail is installed on the industrial switch from the factory. If the DIN-Rail is not installed on the industrial switch, please see the following pictures to install the DIN-Rail on the switch. Follow the steps below to mount the industrial switch.

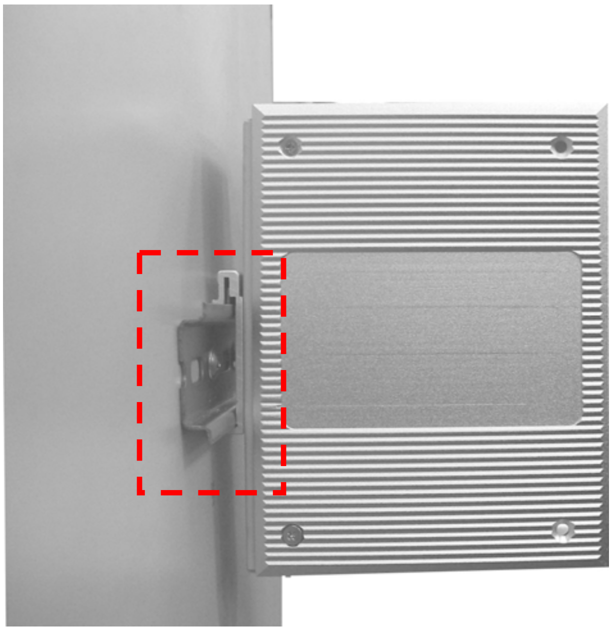


1. Use the screws to install the DIN-Rail on the industrial switch
2. To remove the DIN-Rail, reverse step 1.

1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

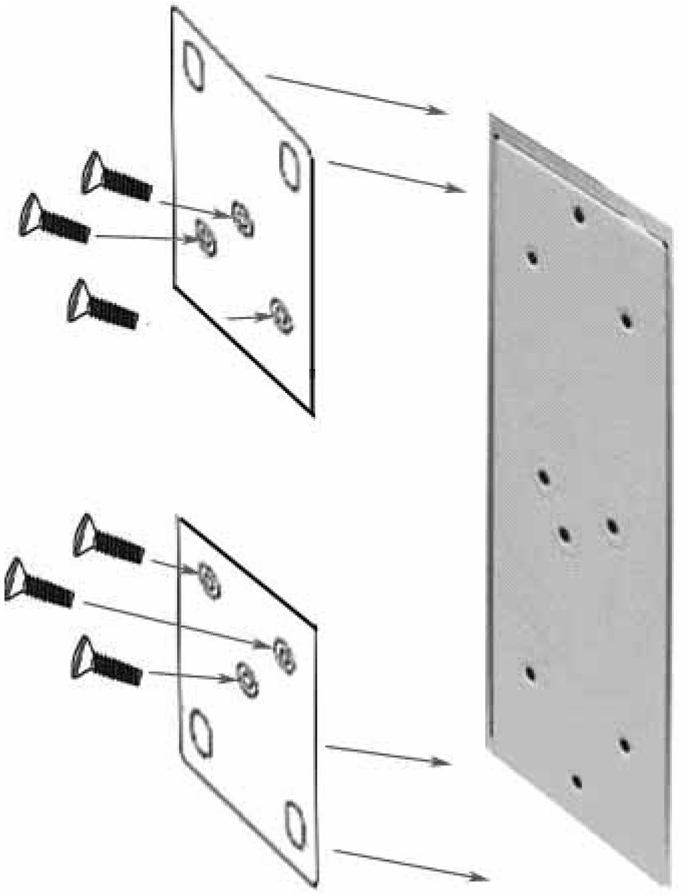


3. Check if the DIN-Rail is tightened on the track.
4. To remove the industrial switch from the track, reverse the steps above.

Wall Mount Plate Mounting

Follow the below steps to mount the industrial switch with wall mount plate.

1. Remove the DIN-Rail from the industrial switch; loosen the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to install the wall mount plate on the industrial switch.
4. Use the hook holes at the corners of the wall mount plate to mount the industrial switch on the wall.
5. To remove the wall mount plate, reverse the steps above.



Installing the wall mount plate on the Industrial switch.

Hardware Installation

In this paragraph, we will describe how to install the 8 10/100TX plus 2 100 FX Managed Industrial Switch.

Installation Steps

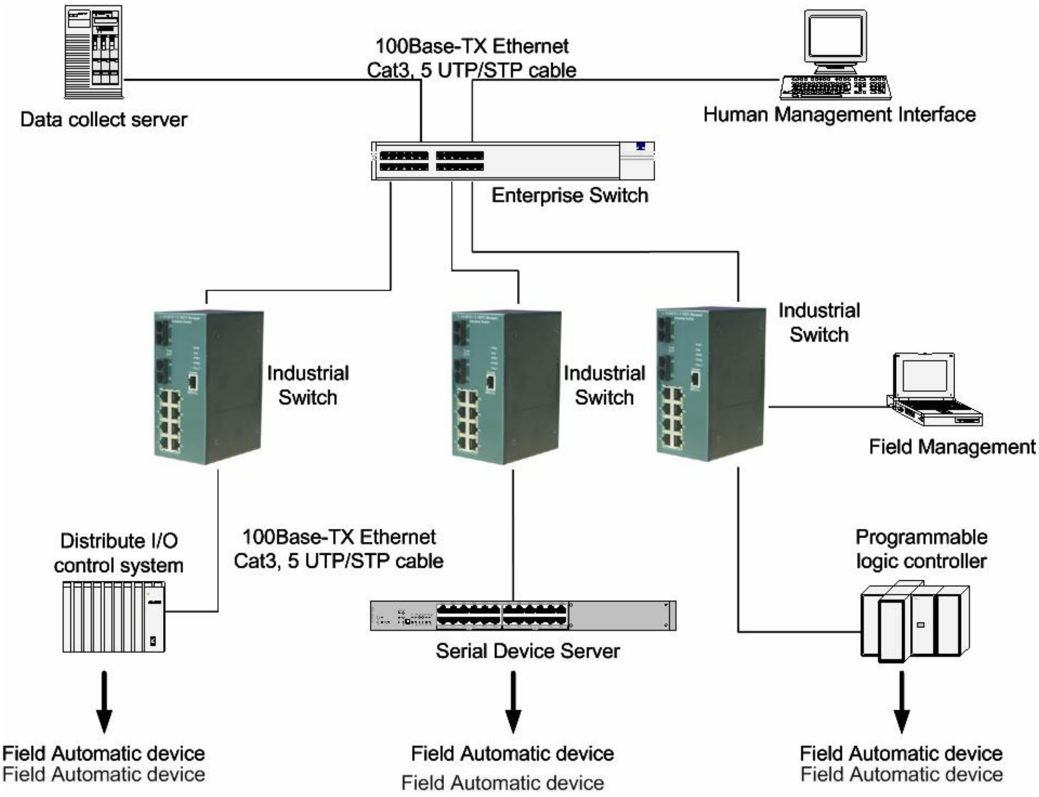
1. Unpack the Industrial switch
2. Check if the DIN-Rail is installed on the Industrial switch. If the DIN-Rail is not screwed on the Industrial switch, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If the user wants to wall mount the Industrial switch, then please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To mount the Industrial switch on the DIN-Rail track or wall, please refer to the **Mounting Installation** section.
4. To apply power on the Industrial switch, please refer to the **Wiring the Power Inputs** section for the information about how to wire the terminal block. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for the indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5 cables for Ethernet connections.
6. Insert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch, PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.

   [NOTE] Make sure that the connected network devices support MDI/MDI-X. If it does not support it, then use a crossover category-5 cable.

7. When all connections are set and LED lights all show normal, the installation is complete.

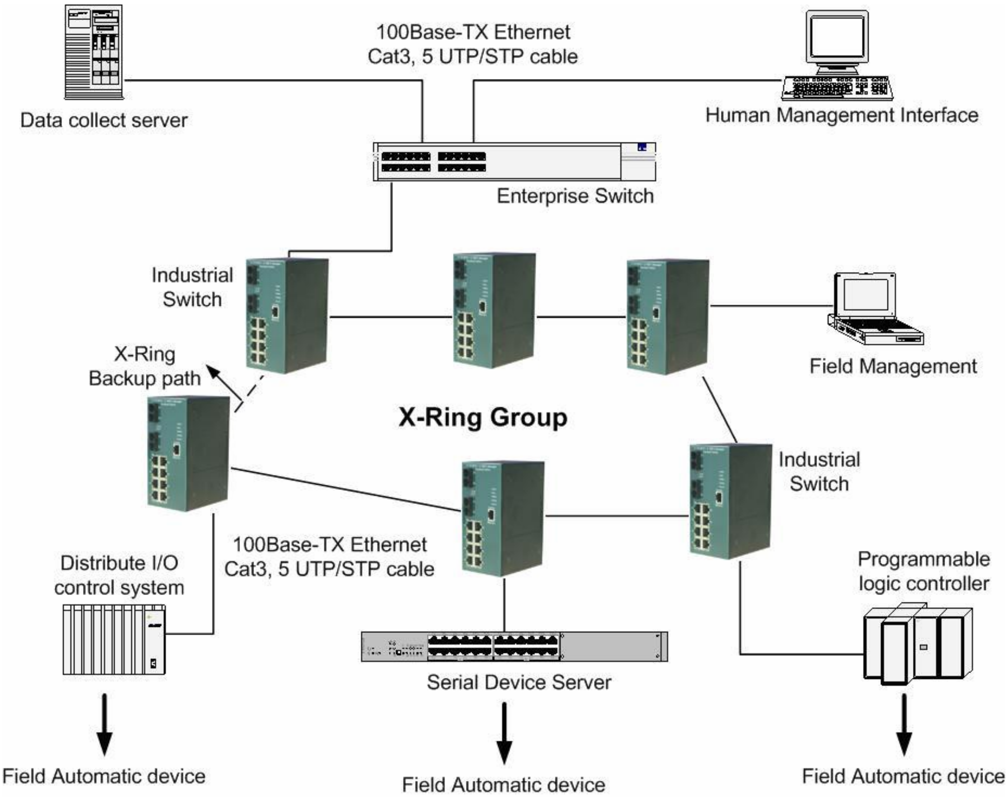
Network Application

This chapter provides some sample applications to help user to have more actual idea of industrial switch function application. A sample application of the industrial switch is as below:



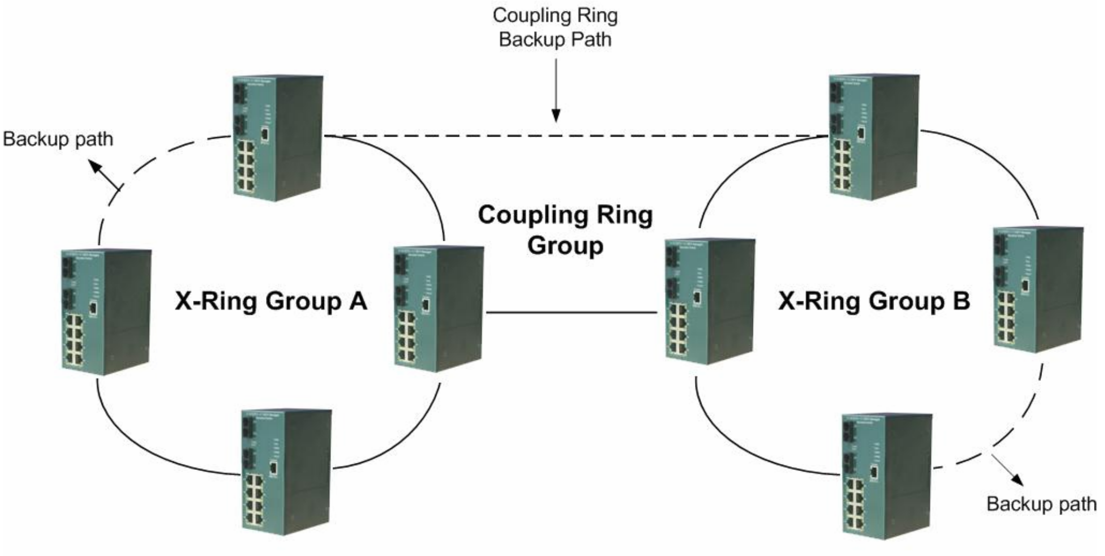
X-Ring Application - Redundancy

The industrial switch supports the X-Ring Redundancy protocol that can help the network system to recover from a network connection failure within 300ms or less, and make the network system more reliable. The X-Ring algorithm is similar to spanning tree protocol (STP) algorithm, but its recovery time is faster than STP and RSTP. The following figure is a sample X-Ring application.



Coupling Ring Application

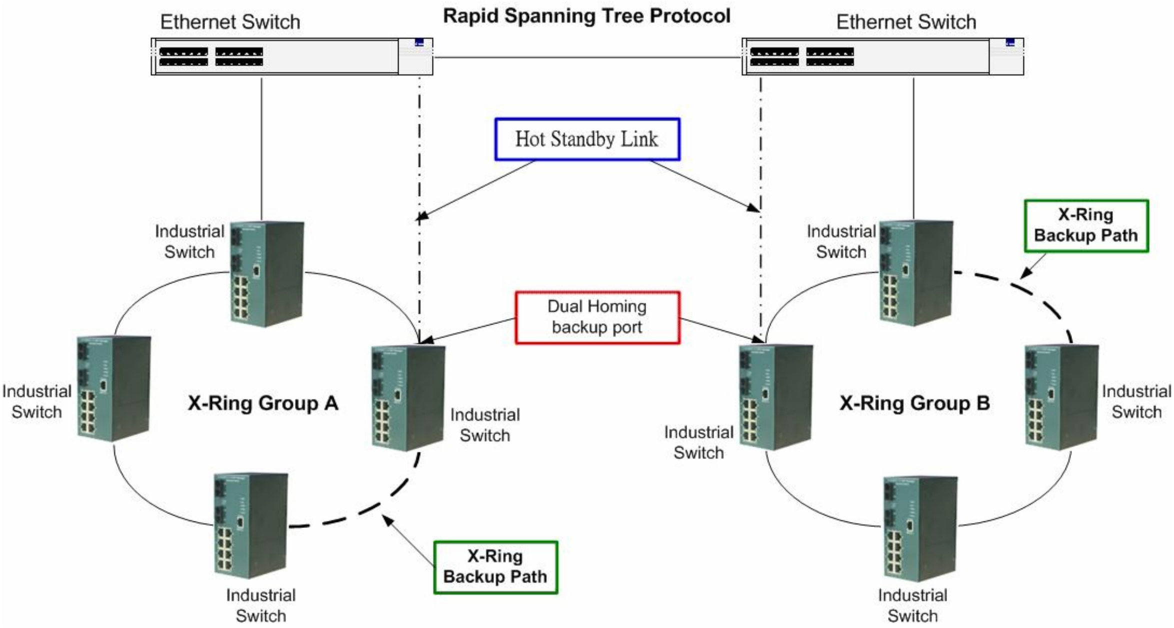
In the network, it may have more than one X-Ring group. By using the coupling ring function, you can connect each X-Ring with the redundant backup. It can ensure the transmissions between two X - Ring groups from failure. The following figure is a sample of a coupling ring application.



Dual Homing Application

A Dual Homing function is to prevent the connection loss from between an X-Ring group and an upper level/core switch. Assign two ports to be the Dual Homing port that is the backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group only has one Dual Homing port.

[NOTE] In Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol (RSTP).



Console Management

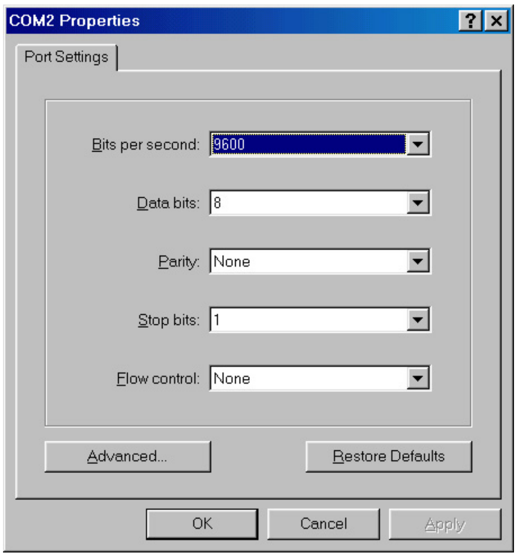
Connecting to the Console Port

The supplied cable - one end is a 9 pin RS-232 connector and the other end is a RJ-45 connector. Attach the end of the RS-232 connector to a PC or terminal and the end of RJ-45 connector to the console port of switch. The connected terminal or PC must support the terminal emulation program.

Login in the Console Interface

When the connection between the Switch and the PC is ready, turn on the PC and run a terminal emulation program such as **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

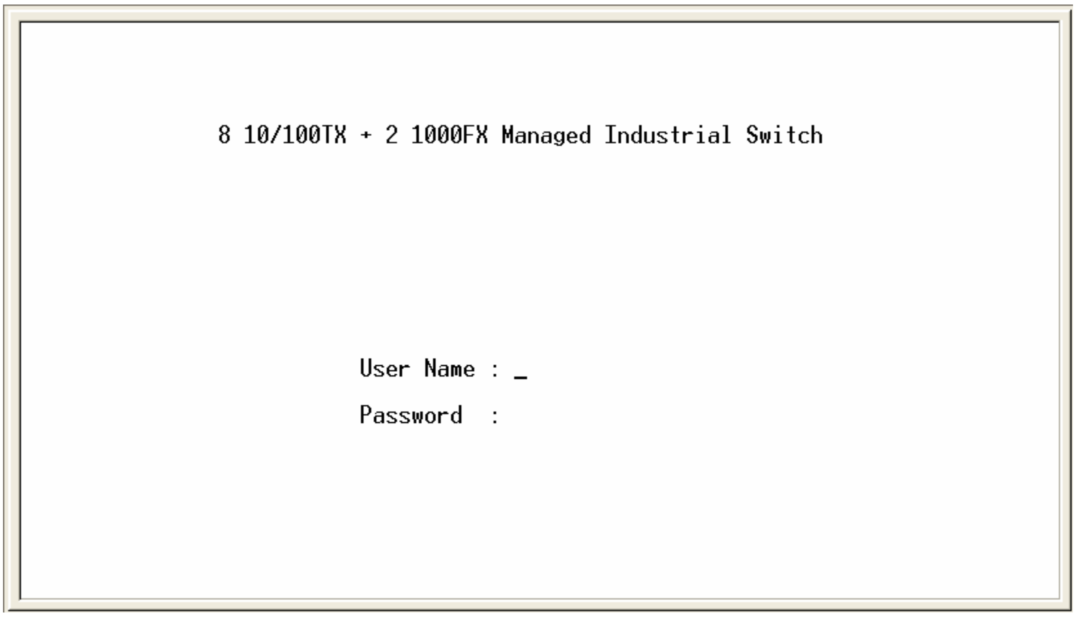
Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

The settings of communication parameters

After setting the parameter settings, click “**OK**“. When the blank screen shows up, press the Enter key to bring up the login prompt. Key in the “**root**“(default value) for the both User name and Password (use **Enter** key to switch), then press the Enter key and the Main Menu of the console management appears. Please see the figure below for the login screen.

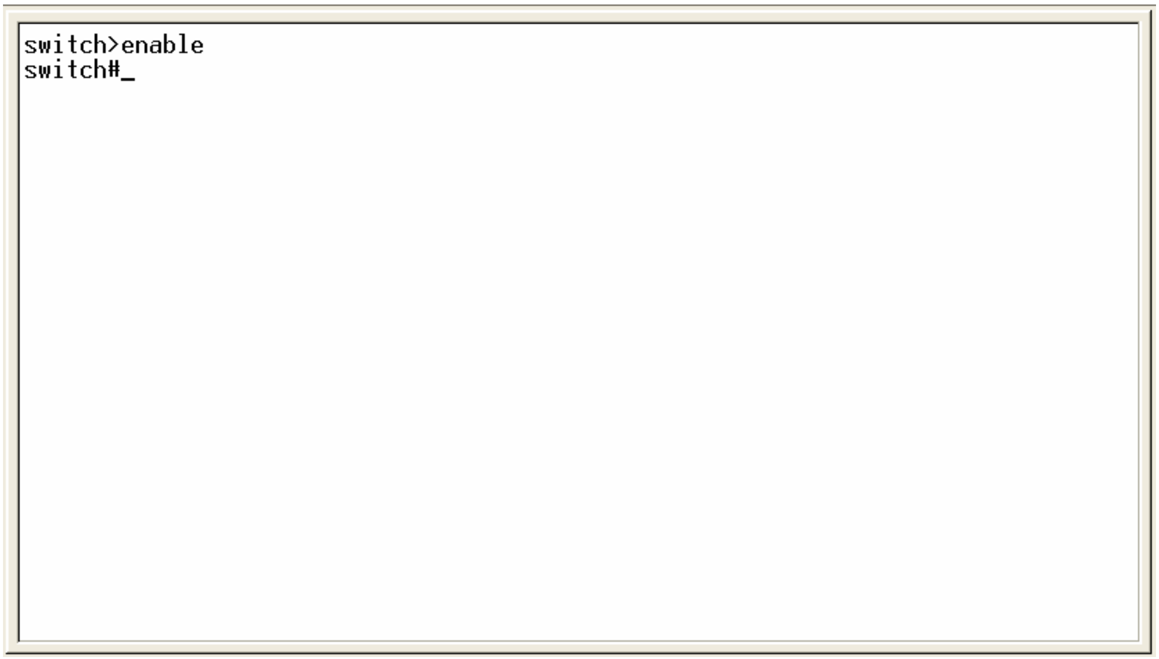


```
8 10/100TX + 2 1000FX Managed Industrial Switch


User Name : _
Password  :
```

Console login interface

CLI Management

The system supports two types of console management – CLI command and Menu selection. After you log in to the system, you will see a command prompt. To enter the CLI management interface, enter the “**enable**” command. (CLI is **Command Line Input)**



```
switch>enable
switch#_
```

CLI command interface

The following table lists the CLI commands and descriptions.

Command Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.

	privileged EXEC mode.			
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

Command Set List

System Command Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
menu	**E**	Enter MENU mode	switch>menu
write memory	**G**	Save user configuration into permanent memory (flash rom)	switch#write memory
system name **[System Name]**	**G**	Configure system name	switch(config)#system name xxx
system location **[System Location]**	**G**	Set switch system location string	switch(config)#system location xxx
system description **[System Description]**	**G**	Set switch system description string	switch(config)#system description xxx

system contact **[System Contact]**	**G**	Set switch system contact window string	switch(config)#system contact xxx
show system-info	**E**	Show system information	switch>show system-info
ip address **[Ip-address] [Subnet-mask] [Gateway]**	**G**	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	**P**	Show IP information of switch	switch#show ip
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	**G**	Halt and perform a cold restart	switch(config)#reload
default	**G**	Restore to default	Switch(config)#default
admin username **[Username]**	**G**	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password **[Password]**	**G**	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	**P**	Show administrator information	switch#show admin
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.100
dhcpserver highip **[High IP]**	**G**	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.200
dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0

dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime **[Hours]**	**G**	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#show dhcpserver clients
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	**G**	Disable DHCP server function	switch(config)#no dhcpserver
security enable	**G**	Enable IP security function	switch(config)#security enable
security http	**G**	Enable IP security of HTTP server	switch(config)#security http
security telnet	**G**	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	**P**	Show the information of IP security	switch#show security
no security	**G**	Disable IP security function	switch(config)#no security
no security http	**G**	Disable IP security of	switch(config)#no security http

		HTTP server	
no security telnet	**G**	Disable IP security of telnet server	switch(config)#no security telnet

Port Command Set

Commands	**Level**	**Description**	**Example**
interface fastEthernet [Portid]	**G**	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	**I**	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	**I**	Enable security of interface	switch(config)#interface fastEthernet 2 (config-if)#security enable

no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to “accept all frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in **[Value]**	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out **[Value]**		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100

		or to 256000 kbps for giga ports, and zero means no limit.	
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state **[Enable | Disable]**	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 (config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 (config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 (config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

Trunk Command Set

Commands	Level	Description	Example
aggregator priority **[1~65535]**	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport **[Port Numbers]**	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group **[GroupID] [Port-list]** **lacp** **workp** **[Workport]**	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group **[GroupID] [Port-list]** **nolacp**	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lacp **[GroupID]**	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group **[GroupID]**	G	Remove a trunk group	switch(config)#no aggreator group 2

VLAN Command Set

Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#vlan database
Vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)# vlanmode portbase or switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan	**V**	Disable VLAN	
Ported based VLAN configuration			
vlan port-based grpname **[Group Name]** **grpid** **[GroupID]** **port** **[PortNumbers]**	**V**	Add new port based VALN	switch(vlan)# vlan port-based grpname test grpid 2 port 2-4
show vlan **[GroupID]** or **show vlan**	**V**	Show VLAN information	switch(vlan)#show vlan 23
no vlan group **[GroupID]**	**V**	Delete port base group ID	switch(vlan)#no vlan group 2
IEEE 802.1Q VLAN			
vlan 8021q name **[GroupName]** **vid** **[VID]**	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#vlan 8021q test vid 22
vlan 8021q port **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this	switch(vlan)#vlan 8021q port 3 access-link untag 33

		command can't be applied.	
vlan 8021q port **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q trunk **[PortNumber]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 access-link untag 33
vlan 8021q trunk **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20
vlan 8021q trunk **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8
show vlan **[GroupID]** or **show vlan**	**V**	Show VLAN information	switch(vlan)#show vlan 23
no vlan group **[GroupID]**	**V**	Delete port base group ID	switch(vlan)#no vlan group 2

Spanning Tree Command Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and	switch(config)# spanning-tree forward-time 20

		learning states last before the port begins forwarding.	
stp-path-cost **[1~200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p **[Auto|True|False]**	**I**	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge	**I**	Admin Edge of STP	switch(config)#interface

[True|False]		priority on this interface.	fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

QOS Command Set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 0 middle
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	Switch#show qos
no qos	G	Disable QoS function	switch(config)#no qos

IGMP Command Set

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

Mac / Filter Table Command Set

Commands	Level	Description	Example
mac-address-table static hwaddr **[MAC]**	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr **[MAC]**	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr **[MAC]**	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678

no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

SNMP Command Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#snmp system-location lab
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#snmp system-contact where
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2cv3
snmp community-strings [Community] right [RO/RW]	G	Add SNMP community string.	switch(config)#snmp community-strings public right rw
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#snmpv3 context-name Test
snmpv3 user [User Name] group	G	Configure the userprofile for SNMPV3 agent.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW

[Group Name] **password** [Authentication Password] [Privacy Password]		Privacy password could be empty.	
snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Configure the access table of SNMPV3 agent	switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1
snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Configure the mibview table of SNMPV3 agent	switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1
show snmp	**P**	Show SNMP configuration	switch#show snmp
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.1.50
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3	switch(config)#no snmpv3 user Test

		agent.	
no snmpv3 access context-name **[Context Name]** **group** **[Group Name]** **security-level** **[NoAuthNoPriv|AuthNoPriv|AuthPriv]** **match-rule** **[Exact|Prifix]** **views** **[Read View Name]** **[Write View Name]** **[Notify View Name]**	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1
no snmpv3 mibview view **[View Name]** **type** **[Excluded|Included]** **sub-oid** **[OID]**	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1

Port Mirroring Command Set

Commands	Level	Description	Example
monitor rx	**G**	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	**G**	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	**P**	Show port monitor information	switch#show monitor

monitor **[RX|TX|Both]**	**I**	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	**I**	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	**I**	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

802.1x Command Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip **[IP address]**	**G**	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport **[port ID]**	**G**	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport **[port ID]**	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816

8021x system sharekey **[ID]**	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid **[words]**	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod **[sec.]**	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod **[sec.]**	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout **[sec.]**	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout **[sec.]**	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20

8021x misc maxrequest **[number]**	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod **[sec.]**	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate **[disable | reject | accept | authorize]**	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	**G**	Disable 802.1x function	switch(config)#no 8021x

TFTP Command Set

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name	switch(config)#backup flash:backup_cfg

		of image.	
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

SystemLog, SMTP and Event Command Sets

Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# systemlog mode both
show systemlog	**E**	Display system log.	Switch>show systemlog
show systemlog	**P**	Show system log client & server information	switch#show systemlog
no systemlog	**G**	Disable systemlog functon	switch(config)#no systemlog
smtp enable	**G**	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	**G**	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	**G**	Configure authentication account	switch(config)#smtp account User

smtp password [password]	**G**	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	**G**	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	**P**	Show the information of SMTP	switch#show smtp
no smtp	**G**	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	**G**	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)#event authentication-failure both
event X - -ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X - ring topology changed event type	switch(config)#event X - -ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	**P**	Show event selection	switch#show event
no event device-cold-start	**G**	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event X - -ring-	**G**	Disable X - ring	switch(config)#no event X - -ring-

topology-change		topology changed event type	topology-change
no event systemlog	**I**	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	**I**	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	**P**	Show system log client & server information	switch#show systemlog

SNTP Command Set

Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch(config)#sntp enable
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	**G**	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	**G**	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip	**G**	Set SNTP server IP, if	switch(config)#sntp ip

[IP]		SNTP function is inactive, this command can't be applied.	192.169.1.1
sntp timezone [Timezone]	**G**	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	**P**	Show SNTP information	switch#show sntp
show sntp timezone	**P**	Show index number of time zone list	switch#show sntp timezone
no sntp	**G**	Disable SNTP function	switch(config)#no sntp
no sntp daylight	**G**	Disable daylight saving time	switch(config)#no sntp daylight

X-ring Command Set

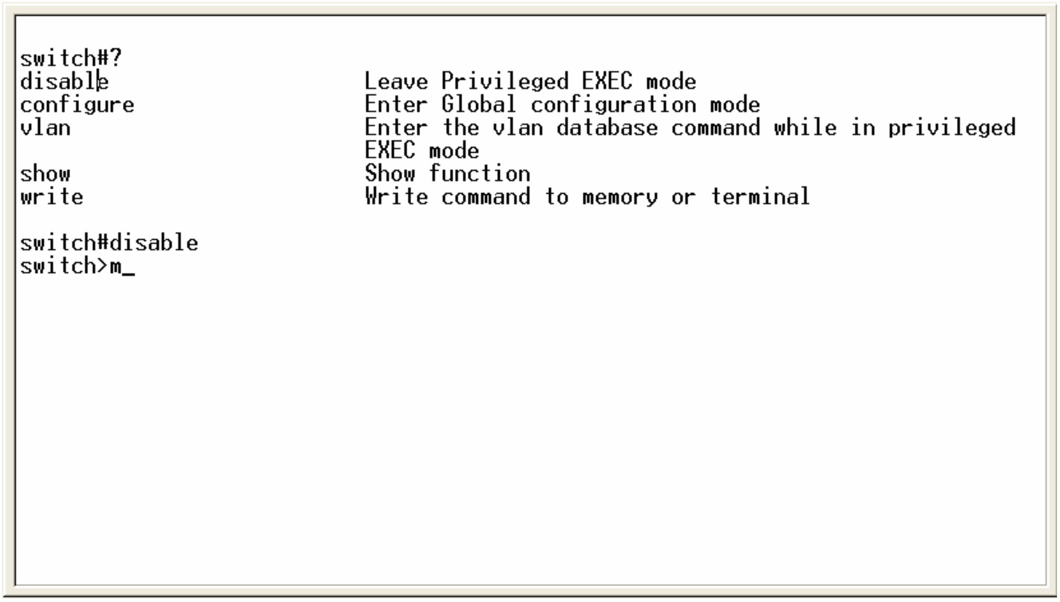
Commands	Level	Description	Example
X-ring enable	**G**	Enable X-ring	switch(config)#Xring enable
X-ring master	**G**	Enable ring master	switch(config)#Xring master
X-ring couplering	**G**	Enable couple ring	switch(config)#Xring couplering
X-ring dualhoming	**G**	Enable dual homing	switch(config)#Xring dualhoming
X-ring ringport [1st Ring Port] [2nd Ring Port]	**G**	Configure 1st/2nd Ring Port	switch(config)#Xring ringport 7 8
X-ring couplingport [Coupling Port]	**G**	Configure Coupling Port	switch(config)#Xring couplingport 1
X-ring controlport [Control Port]	**G**	Configure Control Port	switch(config)#Xring controlport 2
X-ring homingport [Dual Homing Port]	**G**	Configure Dual Homing Port	switch(config)#Xring homingport 3
show X-ring	**P**	Show the information of X - Ring	switch#show Xring
no X-ring	**G**	Disable X-ring	switch(config)#no X ring

no X-ring master	**G**	Disable ring master	switch(config)# no Xring master
no X-ring couplering	**G**	Disable couple ring	switch(config)# no Xring couplering
no X-ring dualhoming	**G**	Disable dual homing	switch(config)# no Xring dualhoming

Main Menu

Input “**disable**” then press **<Enter>** key to quit CLI mode when the prompt symbol is in the state of “**switch#**”.

After the prompt symbol becomes “**switch>**”, input “**Menu**” or “**m**” or “**M**” and press **<Enter>,** the Main Menu interface will appear.



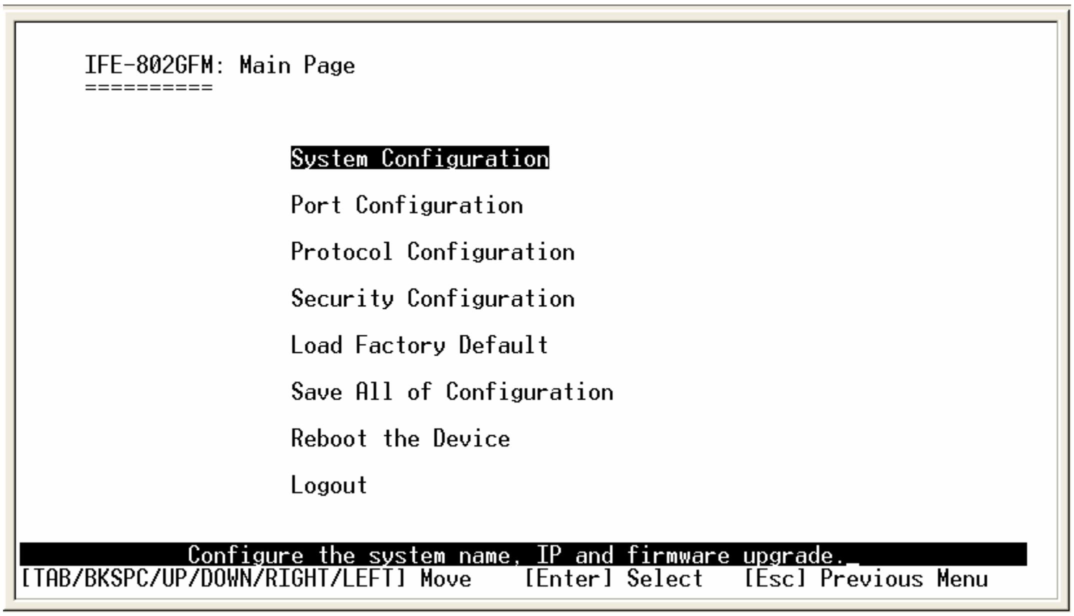
```
switch#?
disable                    Leave Privileged EXEC mode
configure                  Enter Global configuration mode
vlan                       Enter the vlan database command while in privileged
                           EXEC mode
show                       Show function
write                      Write command to memory or terminal

switch#disable
switch>m_
```

Switch to main menu mode from CLI mode

The selections of the main menu are as follows.

- **System Configuration:** Configure system information, IP, DHCP, login security, event logs and firmware update.
- **Port Configuration:** Display port statistic. Configure the port control, trunk, rate limiting and mirroring.
- **Protocol Configuration:** Configure VLAN, RST, SNMP, QoS, SNTP, IGMP, and Super Ring function.
- **Security Configuration:** Configure 802.1X, IP, and Port security function.
- **Load Factory Default:** Reset switch to default configuration.

- **Save All of Configuration:** Save the configuration that user had made in the switch system.
- **Reboot the Device:** Reboot the switch system without reset to the default value.
- **Logout the Device:** Exit the menu line program.



```
    IFE-802GFM: Main Page
    ==========

                        System Configuration

                        Port Configuration

                        Protocol Configuration

                        Security Configuration

                        Load Factory Default

                        Save All of Configuration

                        Reboot the Device

                        Logout

               Configure the system name, IP and firmware upgrade._
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Main menu line interface

- **Control Key description:**

The control keys provided in all menus:

Tab: Move the vernier to next item.

Backspace: Move the vernier to previous item.

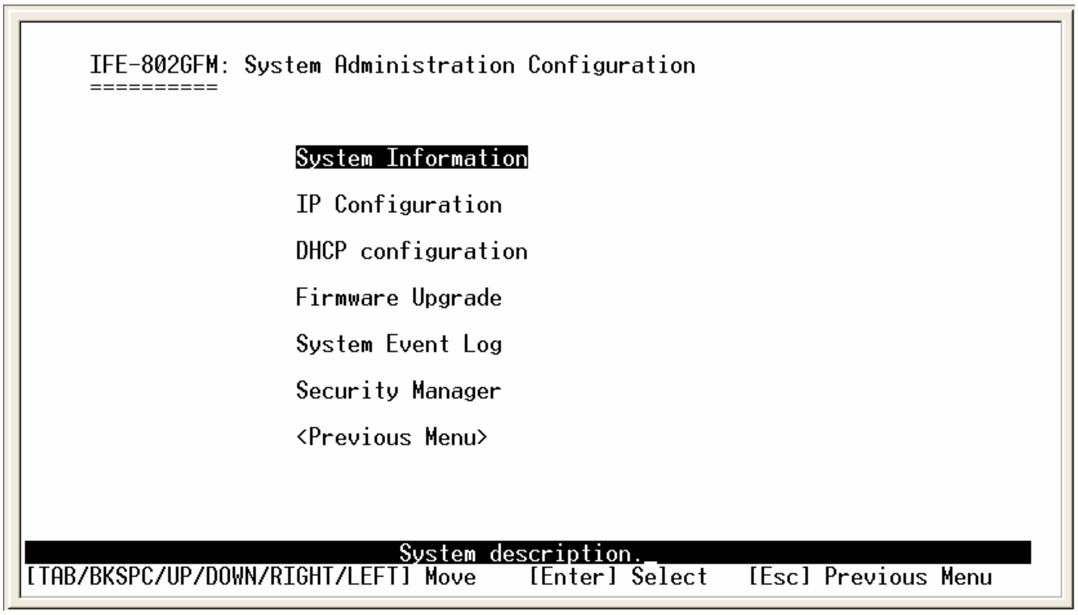
Enter: Select item.

Space: Toggle selected item to next configure or change the value.

Esc: to exit the current action mode.

System Configuration

In System Configuration, you can configure system event log, SMTP, system description, IP, DHCP, login security and firmware update. You can press the “**Tab**” or “**Backspace**” to choose the item, and press “**Enter**” key to select the item.



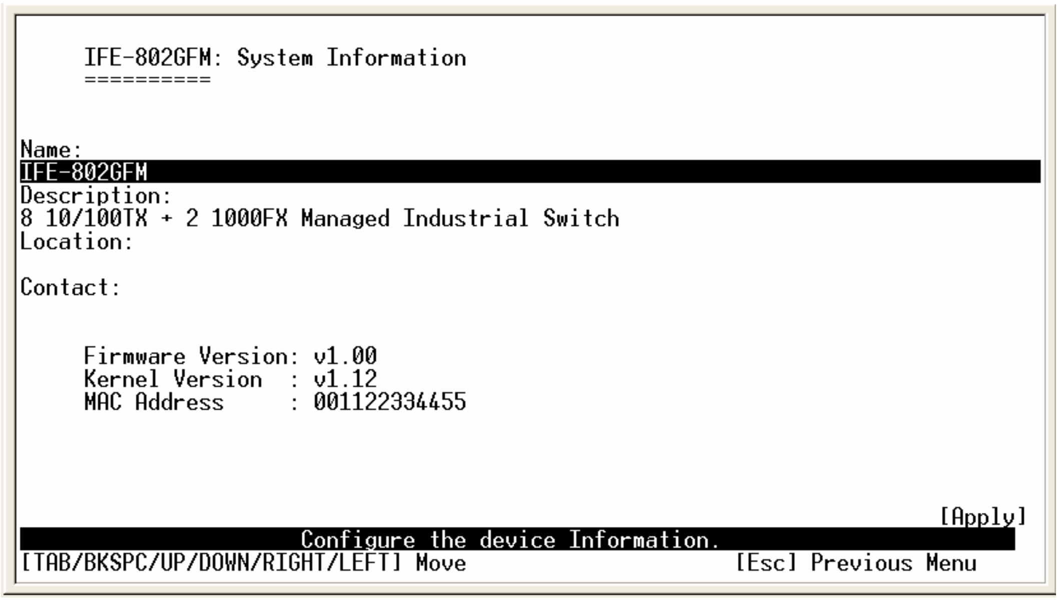
```
     IFE-802GFM: System Administration Configuration
     ==========

                         System Information

                         IP Configuration

                         DHCP configuration

                         Firmware Upgrade

                         System Event Log

                         Security Manager

                         <Previous Menu>



                                               System description._
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Status and Counters main configuration interface

System Information

You can configure the name, description, location, contact of the system. Also, you can view the version of firmware, kernel and MAC address.

1. **Name:** the name of device.
2. **Description:** the name of device type.
3. **Location:** where the device is located.
4. **Contact:** the contact person or information.
5. **Firmware Version:** the switch’s firmware version.
6. **Kernel Version:** the system kernel software version.
7. **MAC Address:** The unique hardware address assigned by manufacturer.
8. Select **<Apply>** to save the configuration



```
     IFE-802GFM: System Information
     ==========

Name:
IFE-802GFM
Description:
8 10/100TX + 2 1000FX Managed Industrial Switch
Location:

Contact:


     Firmware Version: v1.00
     Kernel Version  : v1.12
     MAC Address     : 001122334455




                                                                [Apply]
                       Configure the device Information.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                 [Esc] Previous Menu
```

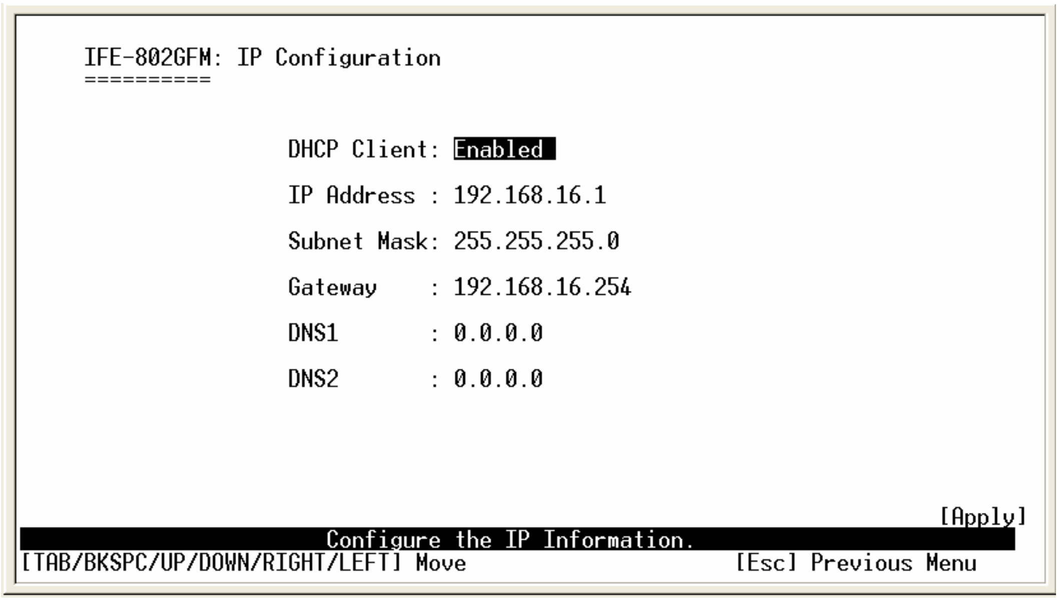
System Description interface

IP Configuration

You can configure the IP for the switch. The system has the default IP address. You can re-configure or use the default value.

1. **DHCP:** disable or enable the DHCP client function. When DHCP function is enabling, you don't need to assign the IP address and subnet mask. The system will be assigned the IP address from the local DHCP server.
2. **IP Address:** assign the switch IP address. **The default IP is 192.168.16.1.**
3. **Subnet Mask:** assign the switch IP subnet mask.
4. **Gateway:** assign the switch gateway. **The default value is 192.168.16.254.**
5. **DNS1:** Short for Domain Name Server an Internet service that translates domain name into IP addresses. Because domain name are alphabetic, they're easier to remember. The Internet is based on IP address. Every time you use a domain name , therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name **www.net.com** might translate to **192.168.1.1**.
6. **DNS2:** The backup for DNS1. When the DNS1 cannot function, the DNS2 can replace DNS1 immediately.
7. Select **<Apply>** action to save the configuration.

[NOTE] Always restart the switch after finished the setup.

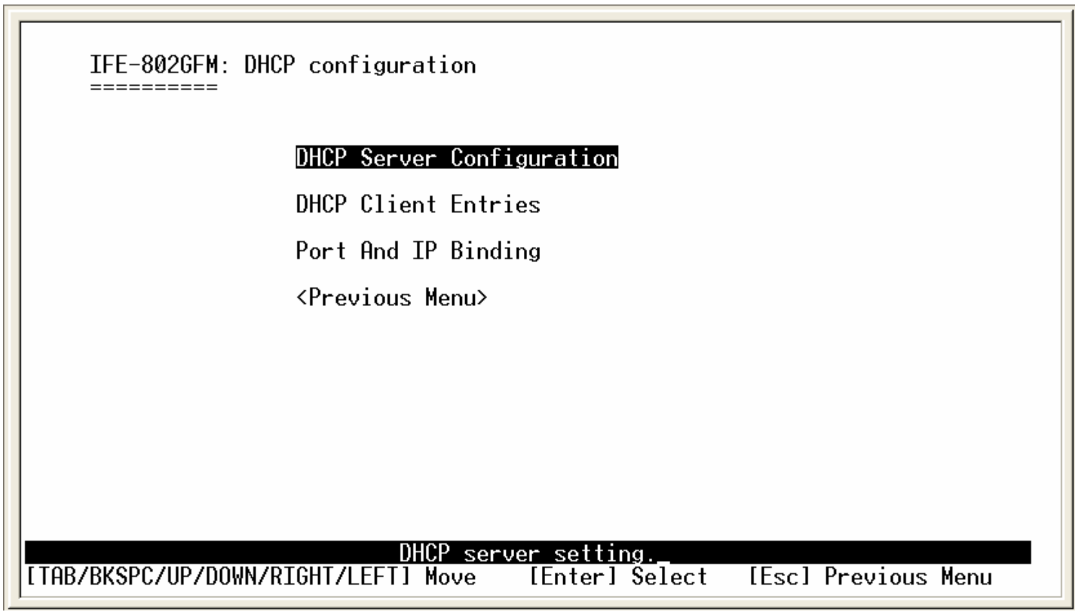


```
    IFE-802GFM: IP Configuration
    ==========

                        DHCP Client: Enabled

                        IP Address : 192.168.16.1

                        Subnet Mask: 255.255.255.0

                        Gateway    : 192.168.16.254

                        DNS1       : 0.0.0.0

                        DNS2       : 0.0.0.0

                                                                  [Apply]
                              Configure the IP Information.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

IP Configuration interface

DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address when it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.



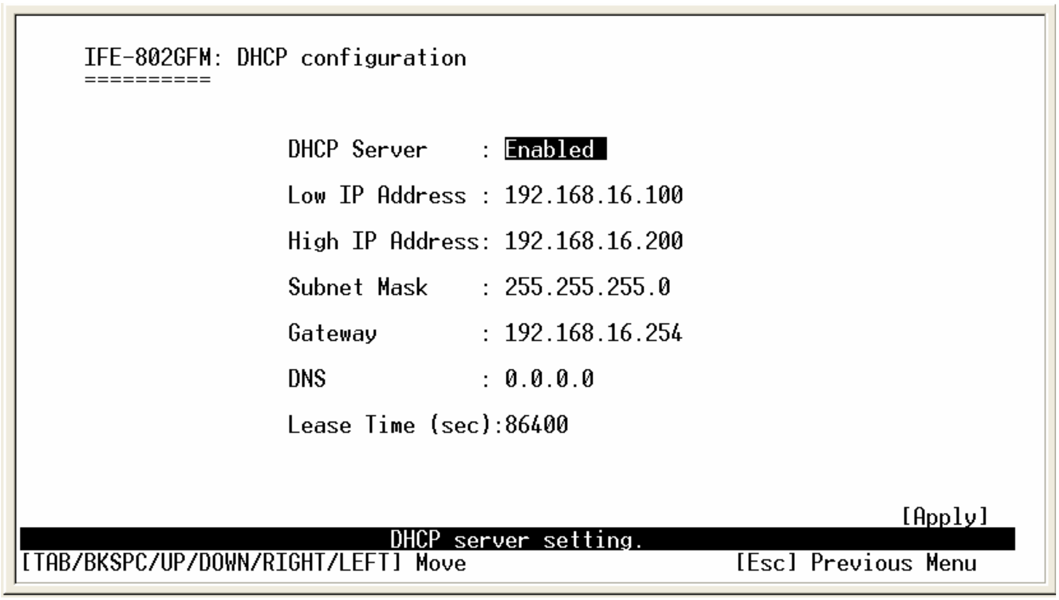
```
IFE-802GFM: DHCP configuration
==========

                DHCP Server Configuration

                DHCP Client Entries

                Port And IP Binding

                <Previous Menu>

                             DHCP server setting._
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

DHCP Configuration interface

DHCP Server Configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assign range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assign range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not be occupied for a long time or the server won’t recognize that the dynamic IP is idle.

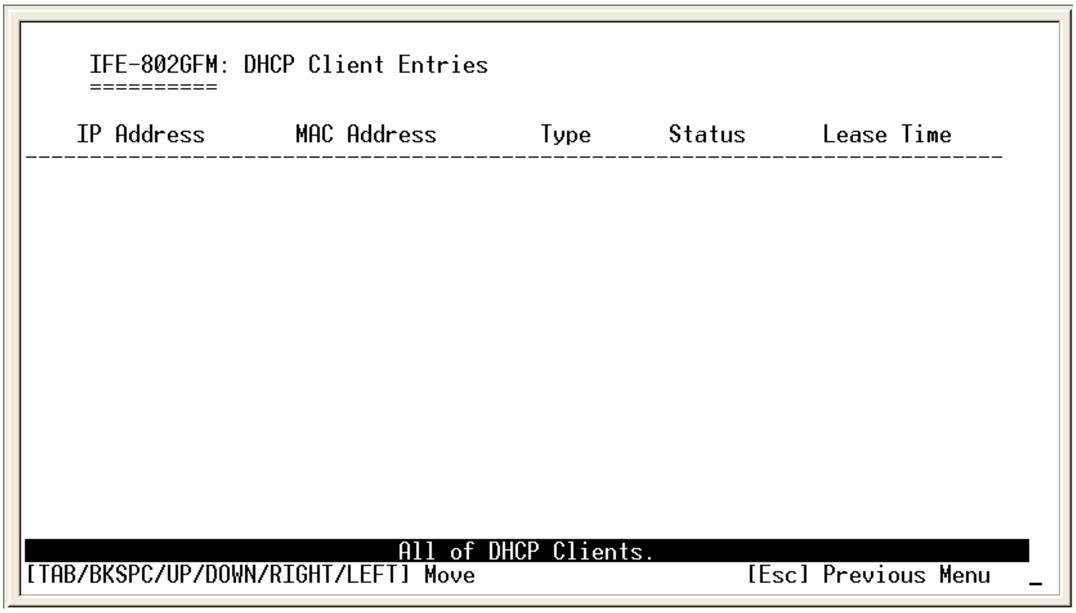


```
IFE-802GFM: DHCP configuration
==========

                    DHCP Server    : Enabled
                    Low IP Address : 192.168.16.100
                    High IP Address: 192.168.16.200
                    Subnet Mask    : 255.255.255.0
                    Gateway        : 192.168.16.254
                    DNS            : 0.0.0.0
                    Lease Time (sec):86400

                                                                  [Apply]
                                 DHCP server setting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

DHCP Server Configuration interface

DHCP Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and display in here.

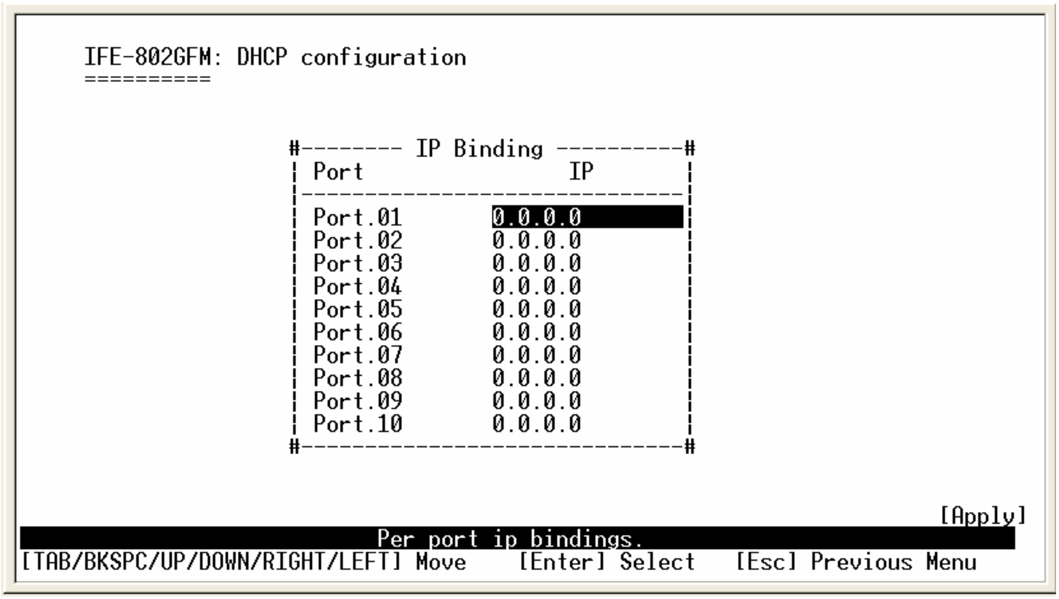


```
IFE-802GFM: DHCP Client Entries
==========

   IP Address       MAC Address       Type      Status      Lease Time
----------------------------------------------------------------------------

                                 All of DHCP Clients.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu  _
```

DHCP Client Entries interface

Port and IP Bindings

You can assign a specific IP address that is the IP in a dynamic IP assigned range to a specific port. When the device is connecting to the port and asking for a dynamic IP assignment, the system will assign the IP address that has been assigned before to the connected device.



```
IFE-802GFM: DHCP configuration
==========

                    #-------- IP Binding ----------#
                    | Port                IP       |
                    |------------------------------|
                    | Port.01       0.0.0.0        |
                    | Port.02       0.0.0.0        |
                    | Port.03       0.0.0.0        |
                    | Port.04       0.0.0.0        |
                    | Port.05       0.0.0.0        |
                    | Port.06       0.0.0.0        |
                    | Port.07       0.0.0.0        |
                    | Port.08       0.0.0.0        |
                    | Port.09       0.0.0.0        |
                    | Port.10       0.0.0.0        |
                    #------------------------------#

                                                              [Apply]
                          Per port ip bindings.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

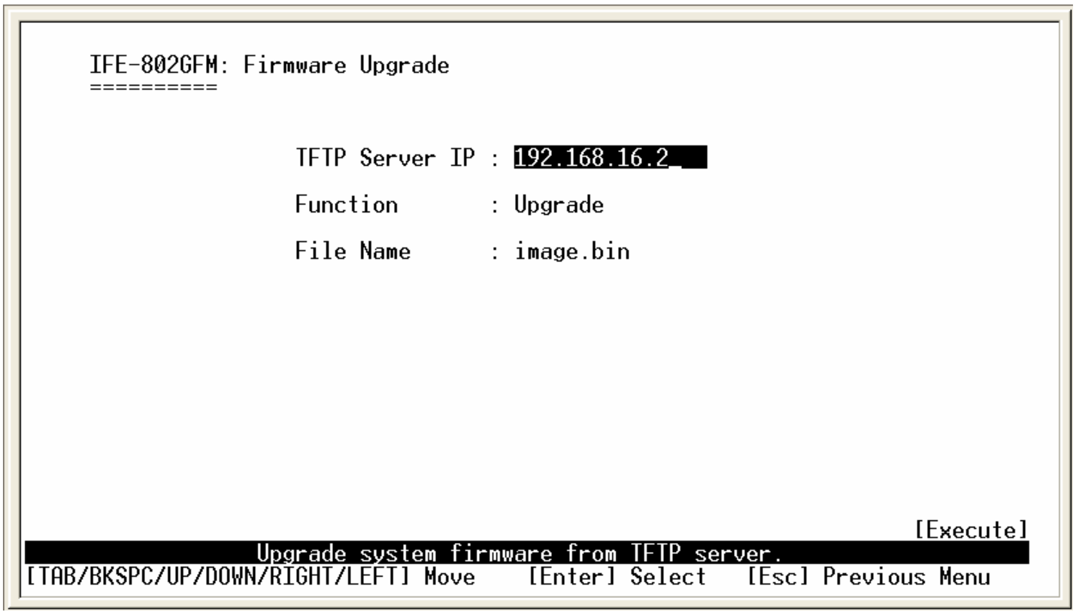
Port and IP Bindings interface

Firmware Update

It allows the user to update the firmware or restore the EEPROM values or backup the current EEPROM values.

1. Start the TFTP server, and copy the new firmware version image file to the TFTP server.
2. **TFTP Server IP:** type the IP of TFTP server.
3. **Function:** the system provides three functions – update, restore, and backup.
   - **Update:** update the firmware.
   - **Restore:** restore the EEPROM value, which is saved in the TFTP server, from TFTP server.
   - **Backup:** save the current EEPROM value to the TFTP server as a backup. The backup file can be restored from the TFTP server when needed.
4. **File Name:** type the image file name.
5. Press “**ESC**” to back to action line.

6. “**Execute**” the configuration.

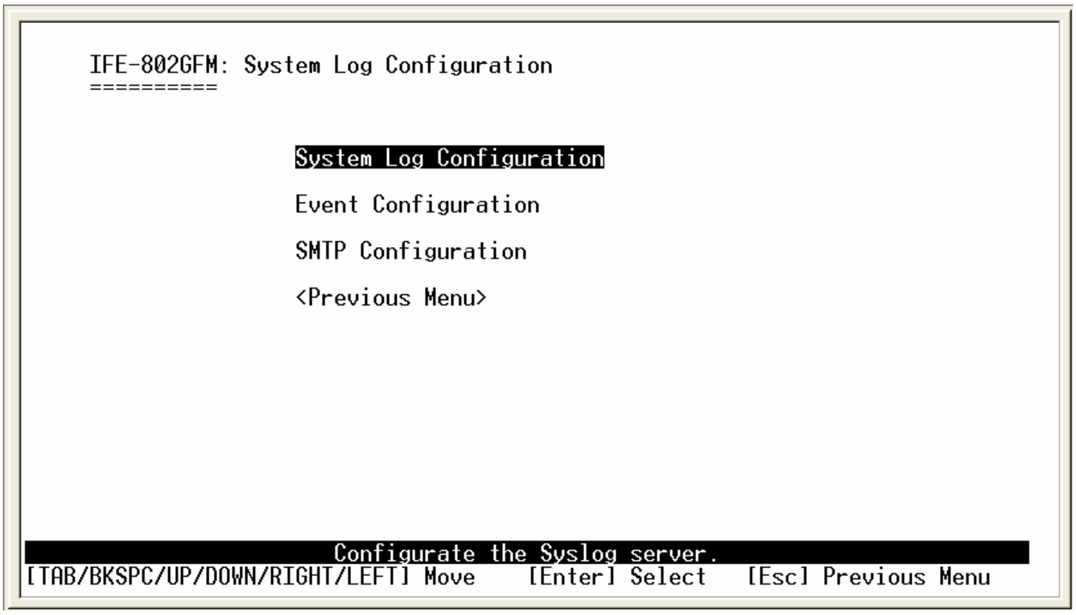


```
IFE-802GFM: Firmware Upgrade
==========

                TFTP Server IP : 192.168.16.2_

                Function       : Upgrade

                File Name      : image.bin










                                                          [Execute]
                  Upgrade system firmware from TFTP server.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Firmware Update interface

System Event Log

Configure the switch as the system log client for receiving and viewing the system log information from system log server.



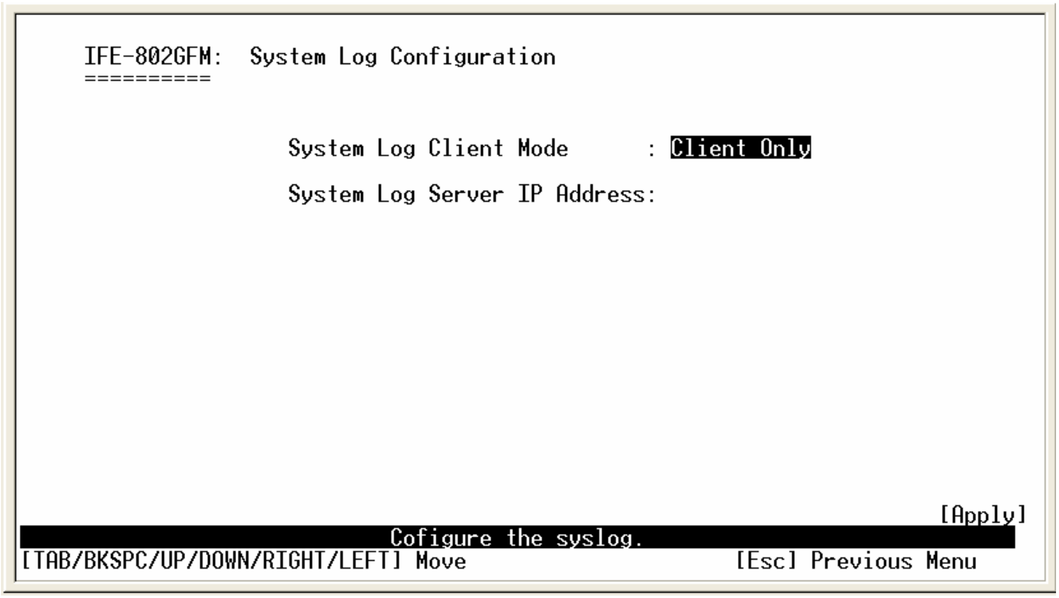
```
IFE-802GFM: System Log Configuration
==========

                System Log Configuration

                Event Configuration

                SMTP Configuration

                <Previous Menu>










                        Configurate the Syslog server.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

System Log Configuration interface

System Log Configuration

Configuring the system event mode that want to be collected and system log server IP.

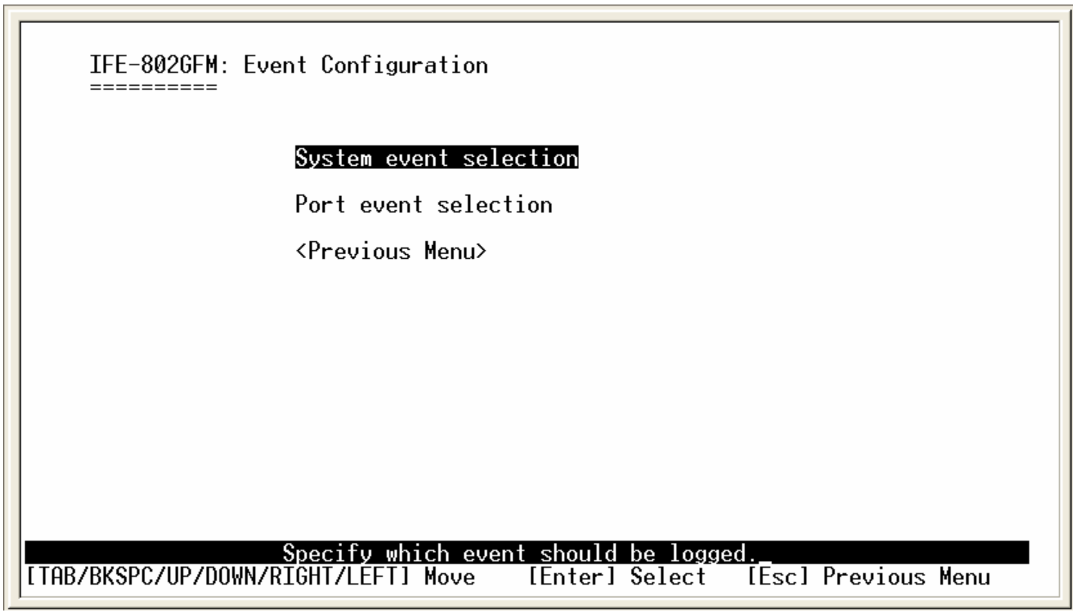
1. **System Log Client Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assigned the system log server IP.
3. Select **<Apply>** to save the configuration.



```
     IFE-802GFM:  System Log Configuration
     ==========

                        System Log Client Mode      : Client Only
                        System Log Server IP Address:



                                                                      [Apply]
                                 Cofigure the syslog.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                  [Esc] Previous Menu
```

System Log Configuration interface

Event Configuration

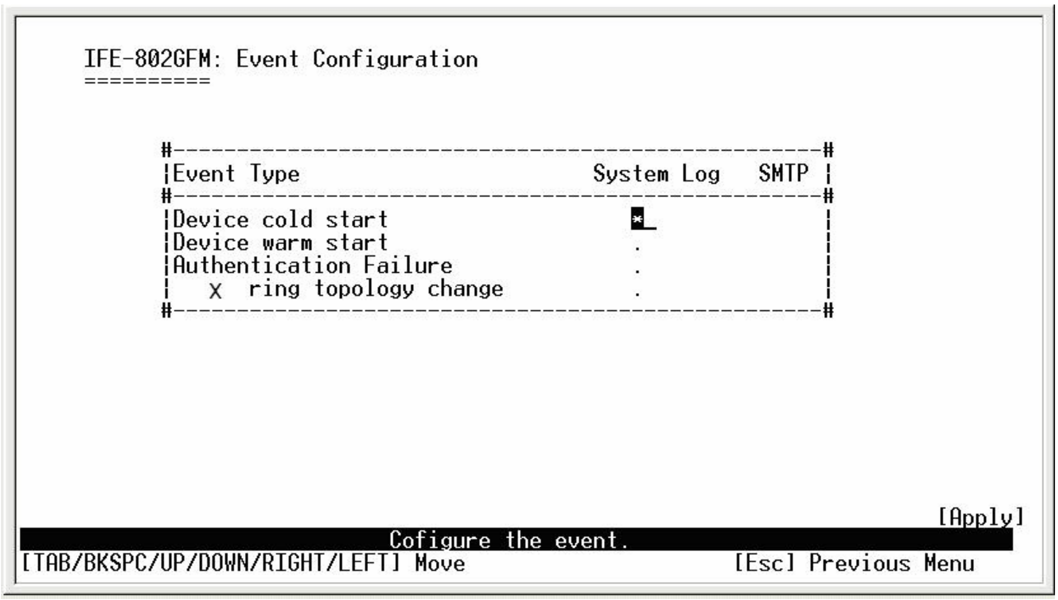


```
IFE-802GFM: Event Configuration
==========

                    System event selection

                    Port event selection

                    <Previous Menu>

                    Specify which event should be logged.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Event Configuration interface

You can select the system log and SMTP events. When selected events occur, the system will send out the log information or alert.

- **Device cold start:** when the device executes cold start action, the system will issue a log event.
- **Device warm start:** when the device executes warm start, the system will issue a log event.
- **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
- **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.
- Select **<Apply>** to save the configuration



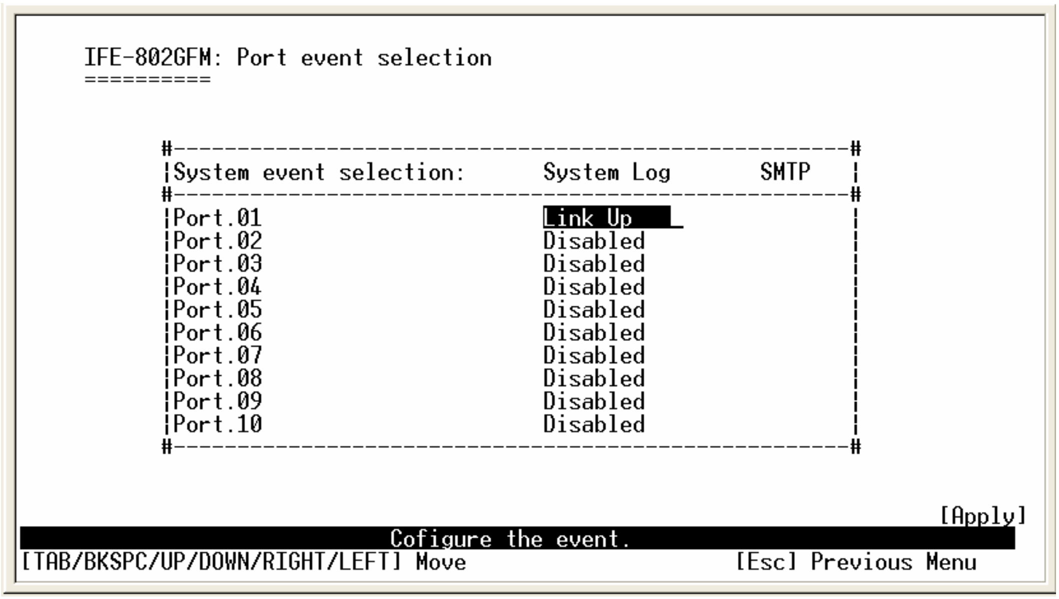
```
IFE-802GFM: Event Configuration
==========

        #-------------------------------------------------#
        |Event Type                    System Log    SMTP |
        #-------------------------------------------------#
        |Device cold start                 *              |
        |Device warm start                 .              |
        |Authentication Failure            .              |
        |   X  ring topology change        .              |
        #-------------------------------------------------#

                                                            [Apply]
                         Cofigure the event.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move            [Esc] Previous Menu
```

System Event Selection interface

Port Event Selection

Select system log and SMTP events of the port

- Select the per port events. Each port has 3 event selections both for system log and SMTP – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected
  - **Link UP:** The system will result a log message when port connection is up only
  - **Link Down:** The system will result a log message when port connection is down only
  - **Link UP & Link Down:** The system will result a log message when port connection is up and down



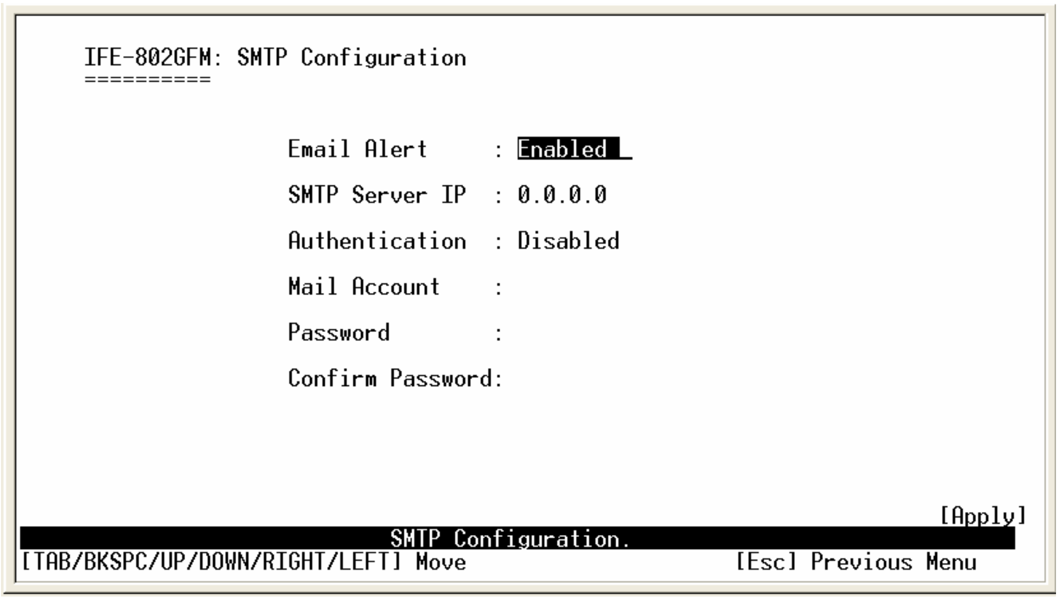
```
     IFE-802GFM: Port event selection
     ==========

            #------------------------------------------------------#
            |System event selection:      System Log       SMTP    |
            #------------------------------------------------------#
            |Port.01                      Link Up                  |
            |Port.02                      Disabled                 |
            |Port.03                      Disabled                 |
            |Port.04                      Disabled                 |
            |Port.05                      Disabled                 |
            |Port.06                      Disabled                 |
            |Port.07                      Disabled                 |
            |Port.08                      Disabled                 |
            |Port.09                      Disabled                 |
            |Port.10                      Disabled                 |
            #------------------------------------------------------#

                                                                     [Apply]
                                Cofigure the event.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                   [Esc] Previous Menu
```

Port Event Selection interface

SMTP Configuration

You can set up the mail server IP, mail account, and account password.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address.
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication.
4. **Mail Account:** set up the email account to receive the alert. Ex: johnadmin@123.com. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.
5. **Password:** The email account password.
6. **Confirm Password:** reconfirm the password.
7. Select **<Apply>** to save the configuration.



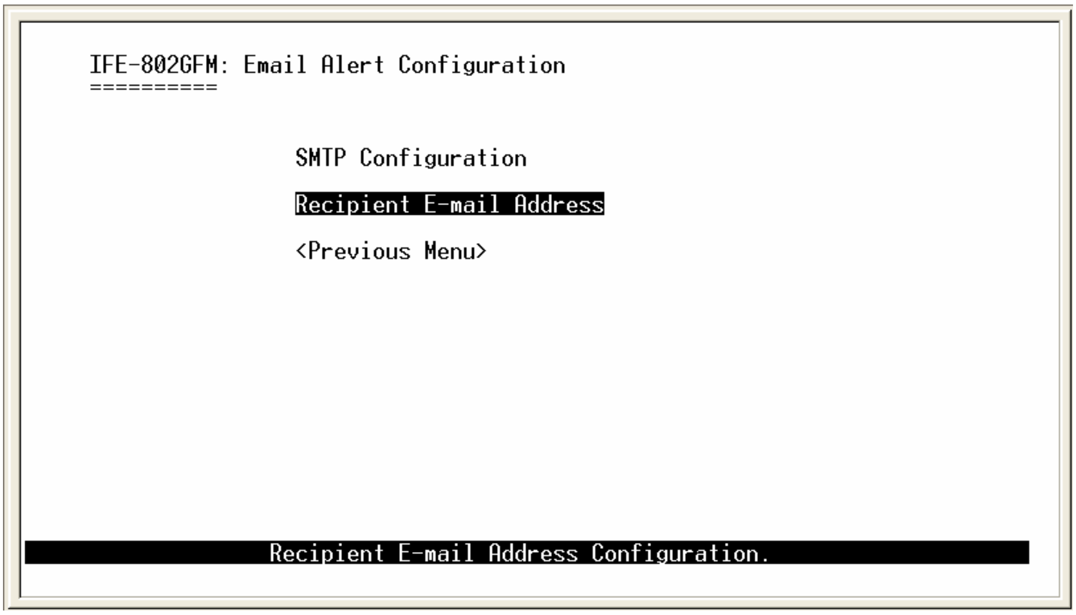
```
IFE-802GFM: SMTP Configuration
==========

                Email Alert     : Enabled
                SMTP Server IP  : 0.0.0.0
                Authentication  : Disabled
                Mail Account    :
                Password        :
                Confirm Password:

                                                          [Apply]
                          SMTP Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move              [Esc] Previous Menu
```

SMTP Configuration interface

Recipient’s email Configuration

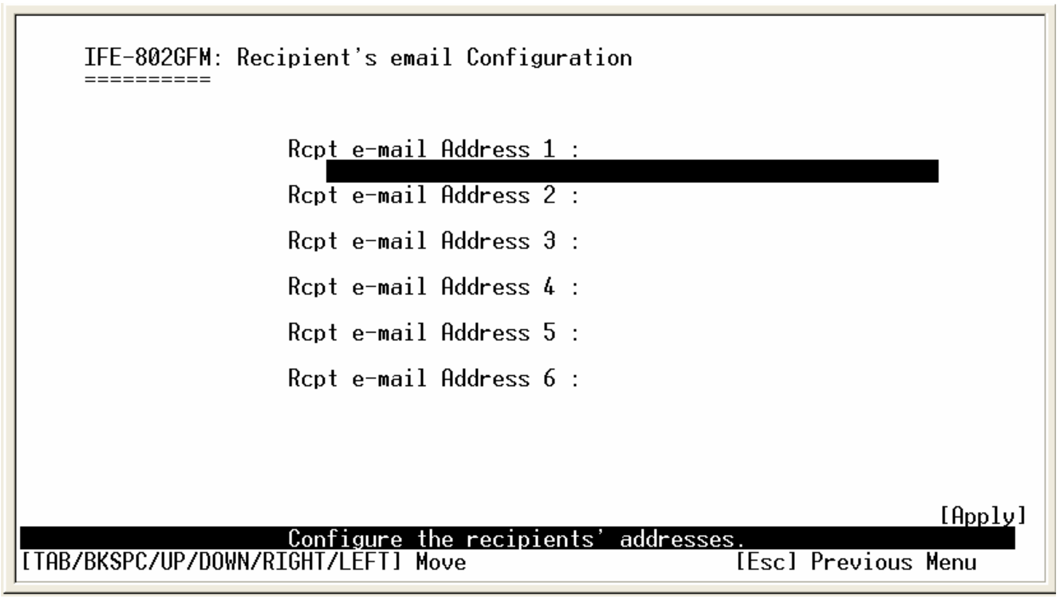
Assign the forwarded email account for receiving the event alert.

- **Rcpt E-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
- Select **<Apply>** to save the configuration



```
IFE-802GFM: Email Alert Configuration
==========

                SMTP Configuration
                Recipient E-mail Address
                <Previous Menu>

                Recipient E-mail Address Configuration.
```

Recipient’s email Configuration interface



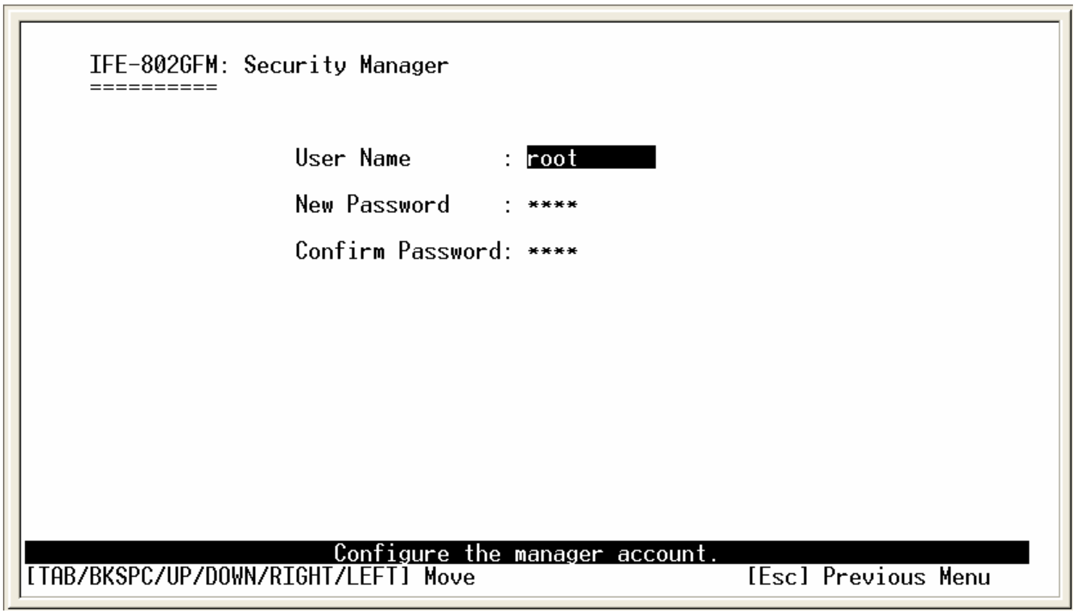
```
IFE-802GFM: Recipient's email Configuration
==========

                    Rcpt e-mail Address 1 :

                    Rcpt e-mail Address 2 :

                    Rcpt e-mail Address 3 :

                    Rcpt e-mail Address 4 :

                    Rcpt e-mail Address 5 :

                    Rcpt e-mail Address 6 :

                                                                      [Apply]
                    Configure the recipients' addresses.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

Recipient's email Configuration interface

Security Manager

You can change the console and web management login user name and password for the security issue.

1. **User Name:** Enter the new user name. The default user name is “root”.
2. **New Password:** enter the new password. The default password is “root”
3. **Confirm Password:** reenter the new password for confirmation.
4. Select **<Apply>** to save the configuration.

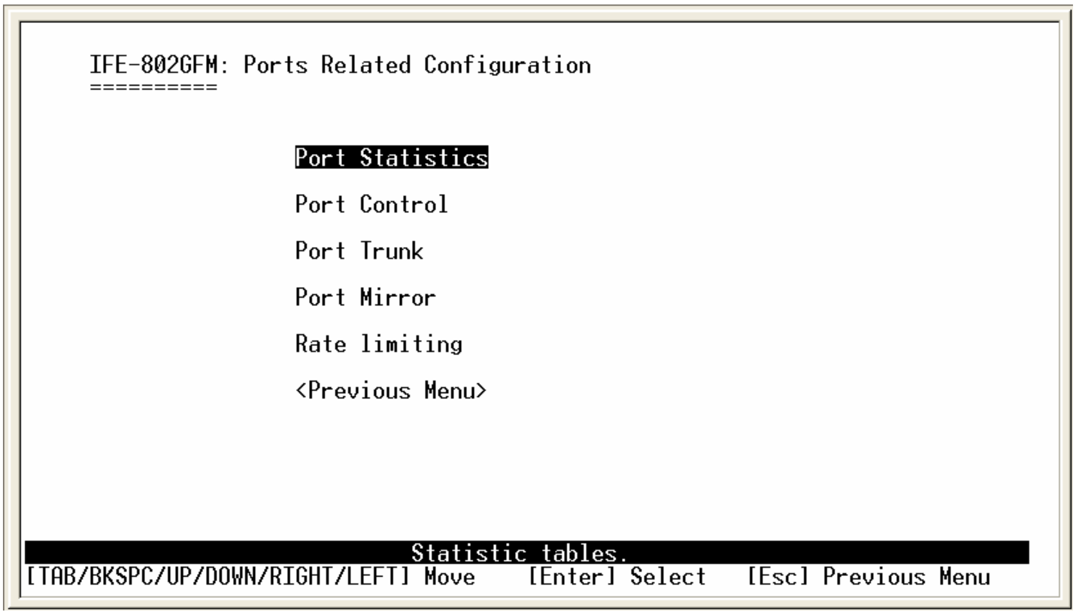


```
IFE-802GFM: Security Manager
==========

                    User Name       : root

                    New Password    : ****

                    Confirm Password: ****



                        Configure the manager account.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

Security Manager interface

Port Configuration

In this section, you can see port counter information, configure port control, mirroring, trunk, and rate limiting.

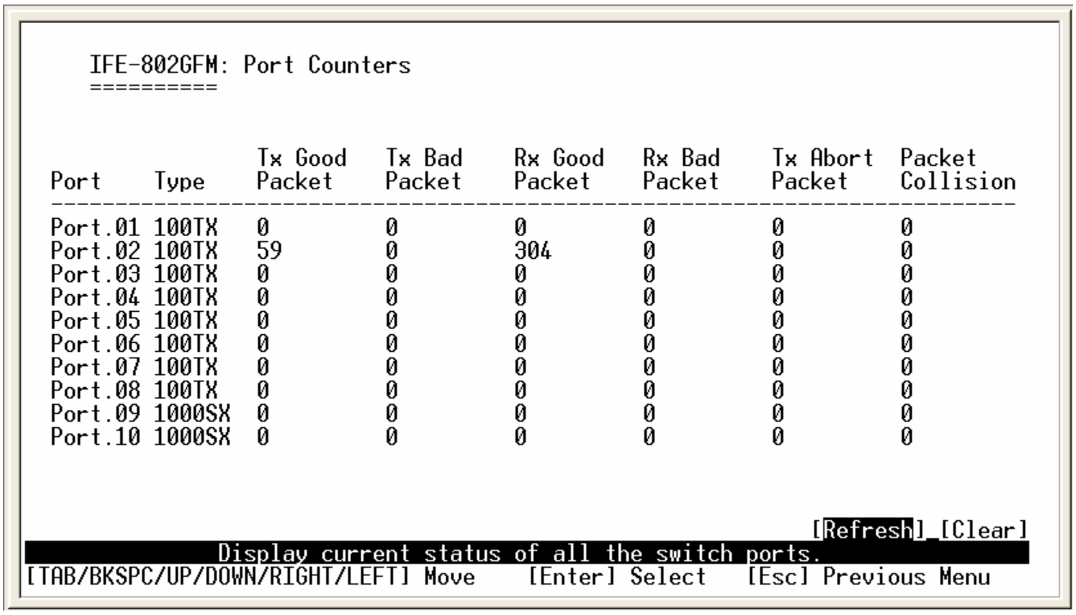


```
     IFE-802GFM: Ports Related Configuration
     ==========

                    Port Statistics

                    Port Control

                    Port Trunk

                    Port Mirror

                    Rate limiting

                    <Previous Menu>




                              Statistic tables.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Port Configuration main interface

Port Counters

It displays the current port counter information. Select the **<Refresh>** action to get newest port counter information. Select the **<Clear>** action to set the port counter information back to 0.



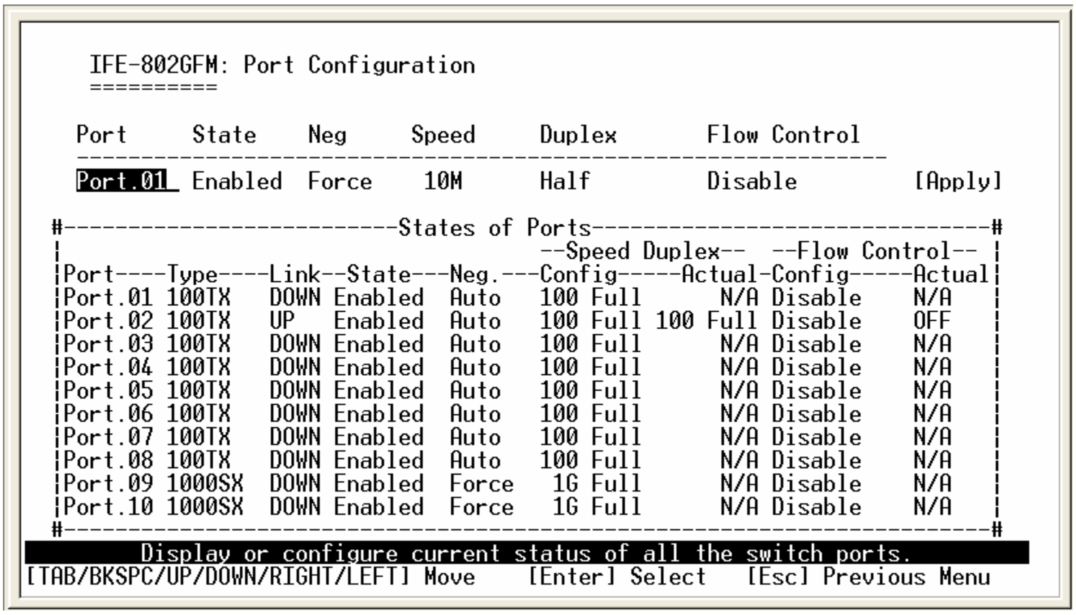
```
    IFE-802GFM: Port Counters
    ==========


                        Tx Good    Tx Bad     Rx Good    Rx Bad     Tx Abort   Packet
Port     Type           Packet     Packet     Packet     Packet     Packet     Collision
---------------------------------------------------------------------------
Port.01 100TX           0          0          0          0          0          0
Port.02 100TX           59         0          304        0          0          0
Port.03 100TX           0          0          0          0          0          0
Port.04 100TX           0          0          0          0          0          0
Port.05 100TX           0          0          0          0          0          0
Port.06 100TX           0          0          0          0          0          0
Port.07 100TX           0          0          0          0          0          0
Port.08 100TX           0          0          0          0          0          0
Port.09 1000SX          0          0          0          0          0          0
Port.10 1000SX          0          0          0          0          0          0


                                                              [Refresh] [Clear]
               Display current status of all the switch ports.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select    [Esc] Previous Menu
```

Port Counter interface

Port Control Configuration

You can set up every port status.

1. Use the "**Tab**" key to move between items.
2. **Port:** select the port to be configured.
3. **State:** Current port status. The port can be set to 'disable' or 'enable' mode. If the port setting is 'disable' then it will not receive or transmit any packet.
4. **Neg:** set the auto-negotiation status of port.
5. **Speed:** set the port link speed.
6. **Duplex:** set the full-duplex or half-duplex mode of the port.
7. **Flow Control:** Set the flow control function as **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Disable**
8. Select the **<Apply>** to save the configuration.



```
     IFE-802GFM: Port Configuration
     ==========

    Port     State    Neg     Speed     Duplex      Flow Control
    ---------------------------------------------------------------
    Port.01  Enabled  Force    10M      Half        Disable         [Apply]

#--------------------------States of Ports------------------------------#
|                                    --Speed Duplex--  --Flow Control-- |
|Port----Type----Link--State---Neg.---Config-----Actual-Config-----Actual|
|Port.01 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.02 100TX   UP   Enabled  Auto   100 Full 100 Full Disable    OFF   |
|Port.03 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.04 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.05 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.06 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.07 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.08 100TX   DOWN Enabled  Auto   100 Full      N/A Disable    N/A   |
|Port.09 1000SX  DOWN Enabled  Force   1G Full      N/A Disable    N/A   |
|Port.10 1000SX  DOWN Enabled  Force   1G Full      N/A Disable    N/A   |
#-----------------------------------------------------------------------#
         Display or configure current status of all the switch ports.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select    [Esc] Previous Menu
```

Port Control Configuration interface

Trunk Configuration

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to seven consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refer to IEEE 802.3ad.

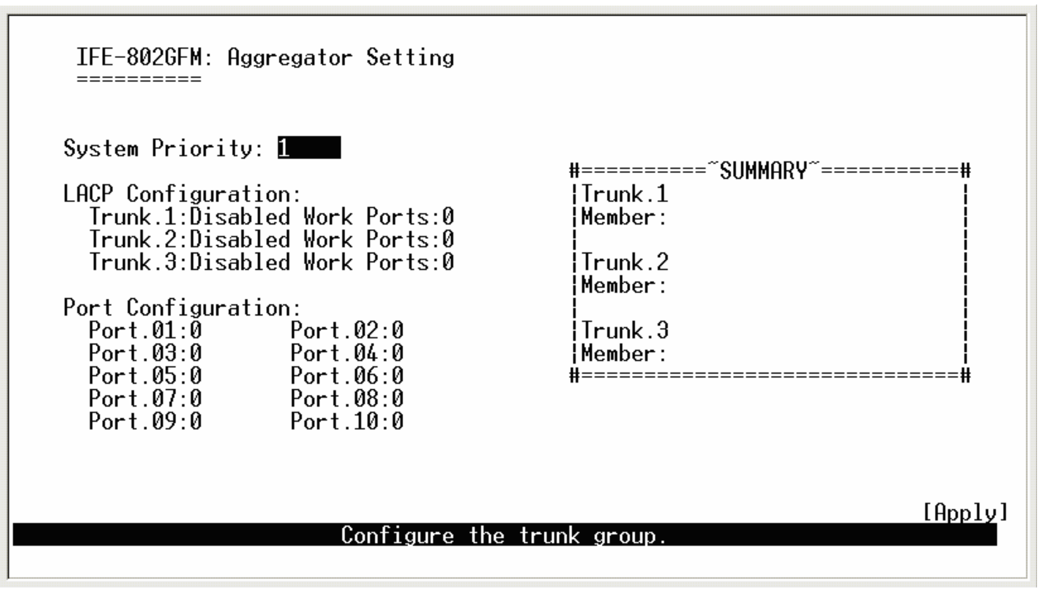
Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **LACP Configuration:** If enable, the group is LACP static trunk group. If disabled, the group is a local static trunk group. All ports support a LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
   - **Trunk Group:** there are three-trunk groups – trunk 1, 2, and 3. You can select

the trunk group and enable the LACP or disable it.

- **Work ports:** select a work port number for the trunk group. The LACP static trunk group work port number cannot be 0.
- **Port Configuration:** to assign the port to the trunk group.

3. Select the ports to join the trunk group.
4. Select the **<Apply>** to save the configuration.
5. You can view the setting information in summary frame.

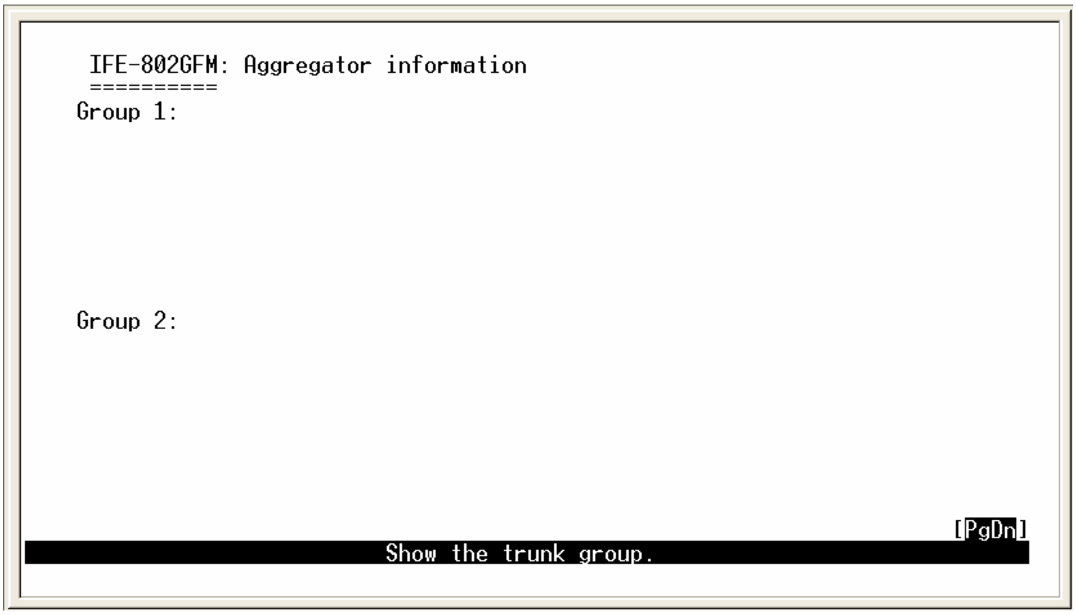


```
IFE-802GFM: Aggregator Setting
==========

System Priority: 1
                                         #==========~SUMMARY~===========#
LACP Configuration:                      |Trunk.1                       |
  Trunk.1:Disabled Work Ports:0          |Member:                       |
  Trunk.2:Disabled Work Ports:0          |                              |
  Trunk.3:Disabled Work Ports:0          |Trunk.2                       |
                                         |Member:                       |
Port Configuration:                      |                              |
  Port.01:0       Port.02:0              |Trunk.3                       |
  Port.03:0       Port.04:0              |Member:                       |
  Port.05:0       Port.06:0              #==============================#
  Port.07:0       Port.08:0
  Port.09:0       Port.10:0


                                                                  [Apply]
                        Configure the trunk group.
```

Trunk Configuration — Aggregator Setting interface

Aggregator Information

When you had setup the LACP aggregator, you will see relate information in here.



```
IFE-802GFM: Aggregator information
==========
Group 1:





Group 2:





                                                                   [PgDn]
                          Show the trunk group.
```

Trunk Configuration – Aggregator Information interface

State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can change the port state activity to **Active** or **Passive**.

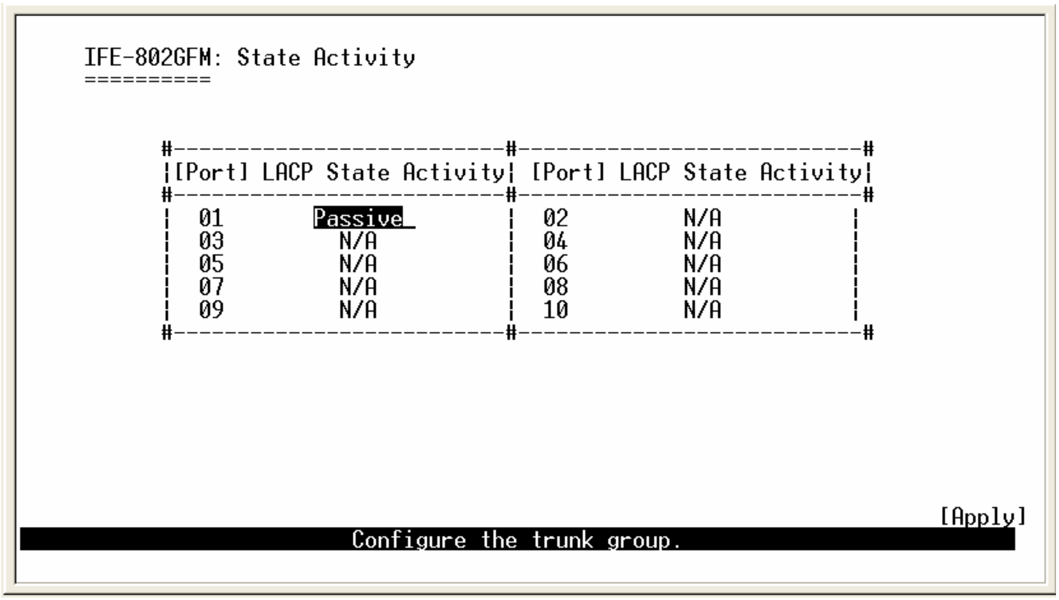
1. **Active:** The port automatically sends LACP protocol packets.
2. **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.
3. Select **<Apply>** to save the configuration.

[NOTE]

a. A link having either two active LACP ports or one active port can perform dynamic LACP trunking.

b. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for and LACP protocol packet from the opposite device.

c. If you are an active LACP's actor, when you select a trunking port, the active status will be created automatically.



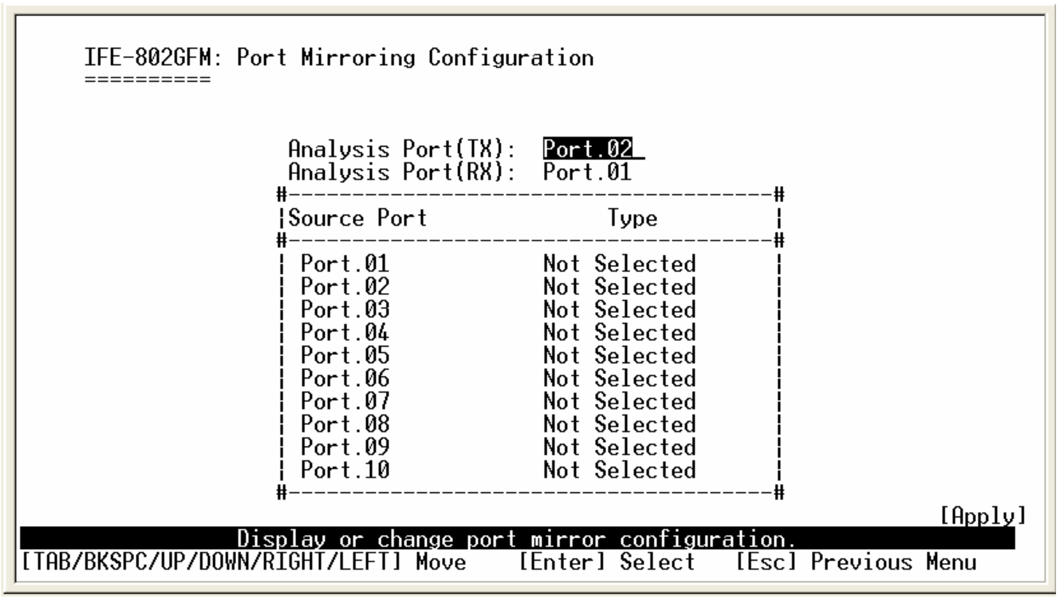
```
IFE-802GFM: State Activity
==========

#--------------------------#--------------------------#
|[Port] LACP State Activity| [Port] LACP State Activity|
#--------------------------#--------------------------#
|  01       Passive        |  02        N/A           |
|  03         N/A          |  04        N/A           |
|  05         N/A          |  06        N/A           |
|  07         N/A          |  08        N/A           |
|  09         N/A          |  10        N/A           |
#--------------------------#--------------------------#

                                                  [Apply]
                  Configure the trunk group.
```

Trunk Configuration – State Activity

Port Mirroring Configuration

The port mirroring is a method for monitor traffic of switched networks. The specific port can monitor traffic through the mirror ports. The monitored ports in or out traffic will be duplicated into the monitoring port.

1. **Analysis Port (TX):** It is a mirror port that can be used to see all monitored port traffic. You can connect the mirror port to a LAN analyzer.
2. **Analysis Port (RX):** Set the destination port of the mirroring packet. All of the packets of the mirroring port will be duplicated and sent to the Analysis port.
3. **Source Port (TX/RX)**: select the port to be monitored. You can choose which port to be monitored - only one port can be selected in the mirror mode.
   - **RX:** RX packet only
   - **TX:** TX packet only
   - **Both:** RX and TX packet
4. Select **<Apply>** to save the configuration.



```
     IFE-802GFM: Port Mirroring Configuration
     ==========

                         Analysis Port(TX):  Port.02
                         Analysis Port(RX):  Port.01
                        #--------------------------------------#
                        |Source Port              Type         |
                        #--------------------------------------#
                        | Port.01             Not Selected     |
                        | Port.02             Not Selected     |
                        | Port.03             Not Selected     |
                        | Port.04             Not Selected     |
                        | Port.05             Not Selected     |
                        | Port.06             Not Selected     |
                        | Port.07             Not Selected     |
                        | Port.08             Not Selected     |
                        | Port.09             Not Selected     |
                        | Port.10             Not Selected     |
                        #--------------------------------------#
                                                                    [Apply]
                    Display or change port mirror configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Port Mirroring interface

Rate Limiting

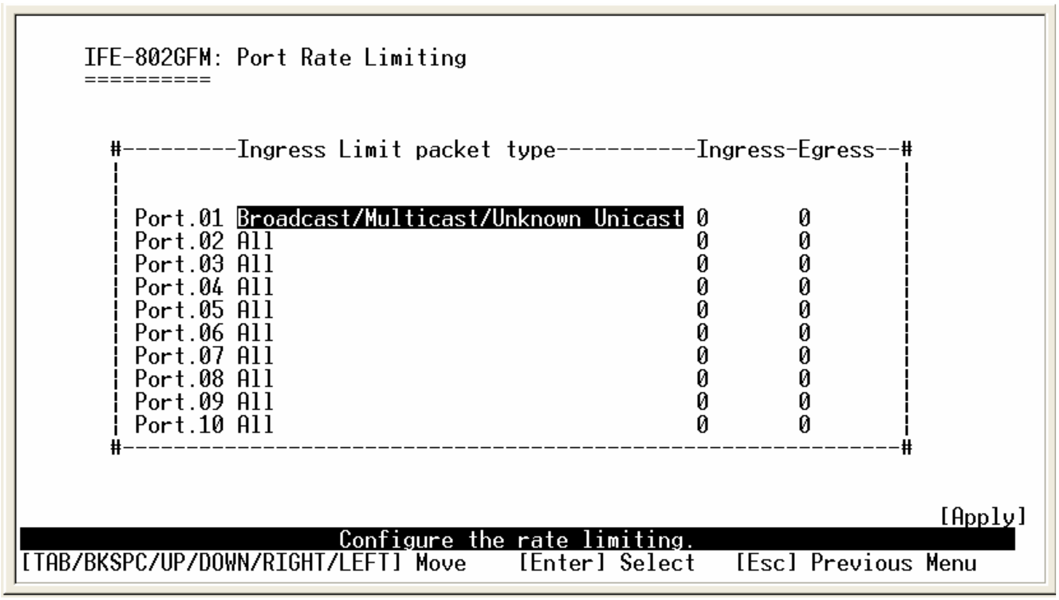
You can set up every port’s bandwidth rate and packet limitation type.

- **Ingress Limit Packet type:** select the packet type which the user would like to filter. The packet types have all type packet, broadcast packet only, broadcast/multicast packet and broadcast/multicast/flooded unicast packet. The broadcast packet only, broadcast/multicast packet and broadcast/multicast/flooded unicast packet are only for ingress packet. The egress rate only supports all type packets.
- All the ports support port ingress and egress rate control. For example, assume port

1 is 10Mbps, users can set the effective egress rate to 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by the packet counter to meet the specified rate.

- **Ingress:** enter the port effective ingress rate. The default value is “0”.
- **Egress:** enter the port effective egress rate. The default value is “0”.

- Select **<Apply>** to save the configuration.

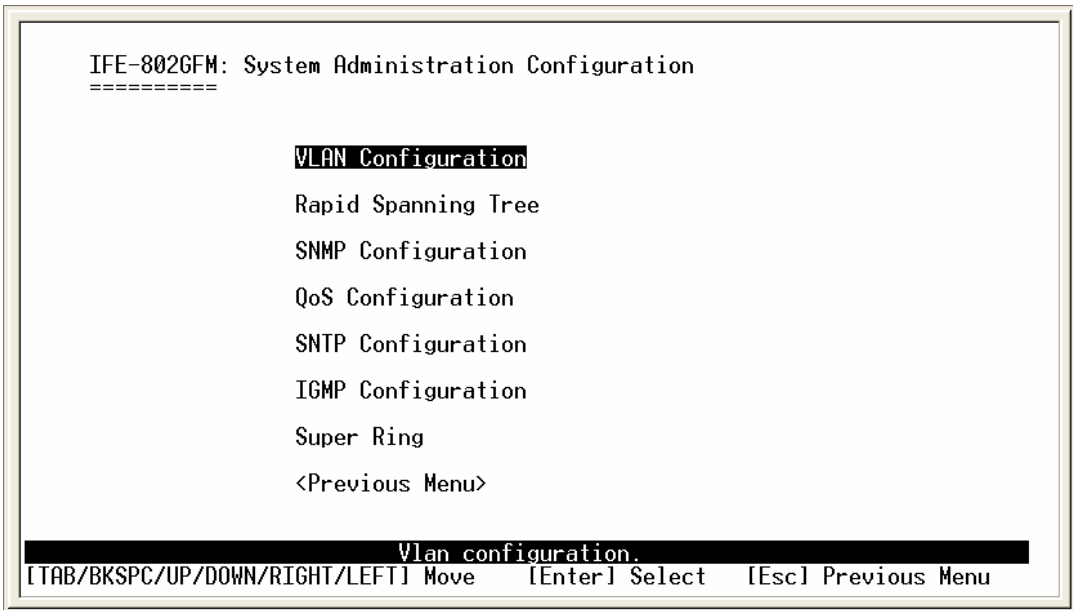


```
IFE-802GFM: Port Rate Limiting
==========

  #---------Ingress Limit packet type-----------Ingress-Egress--#
  |                                                             |
  |                                                             |
  | Port.01 Broadcast/Multicast/Unknown Unicast 0       0       |
  | Port.02 All                                 0       0       |
  | Port.03 All                                 0       0       |
  | Port.04 All                                 0       0       |
  | Port.05 All                                 0       0       |
  | Port.06 All                                 0       0       |
  | Port.07 All                                 0       0       |
  | Port.08 All                                 0       0       |
  | Port.09 All                                 0       0       |
  | Port.10 All                                 0       0       |
  #-------------------------------------------------------------#

                                                               [Apply]
                        Configure the rate limiting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Rate Limiting interface

Protocol Configuration

In this section, you can configure VLAN, RST, SNMP, SNTP, QoS, IGMP, and X-ring.

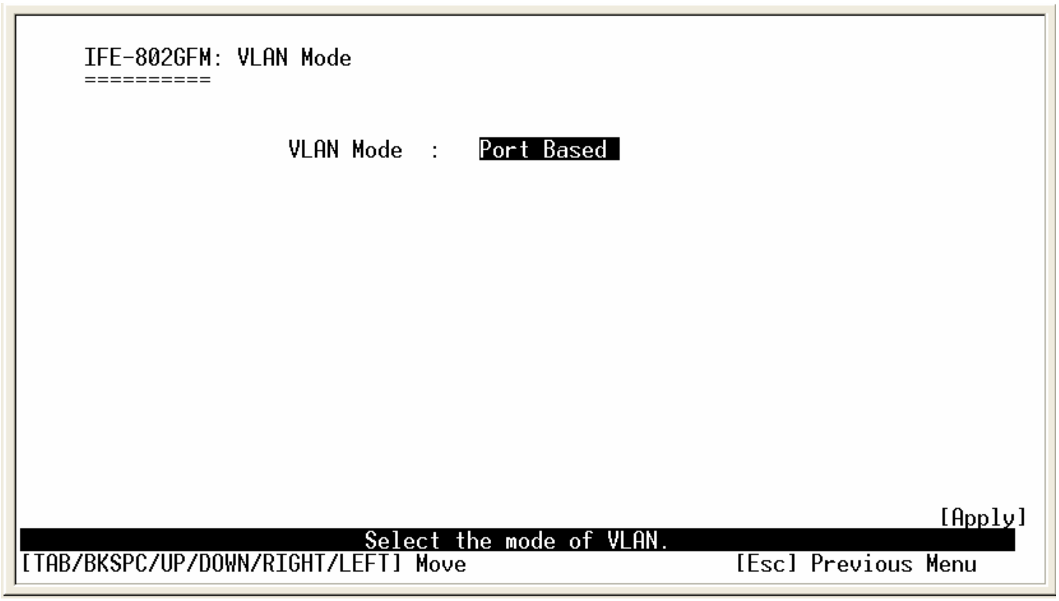


```
IFE-802GFM: System Administration Configuration
==========

                VLAN Configuration
                Rapid Spanning Tree
                SNMP Configuration
                QoS Configuration
                SNTP Configuration
                IGMP Configuration
                Super Ring
                <Previous Menu>

                        Vlan configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Protocol Configuration interface

VLAN Configuration

The VLAN Configuration provides two VLAN modes – Port Based and 802.1Q. You need to select the VLAN mode for the VLAN detail configuration. Use the **Space** key to switch the VLAN mode selection. After selecting the VLAN mode, **<Apply>** the selection. Press the **ESC** key to exit the VLAN Mode Selection interface.

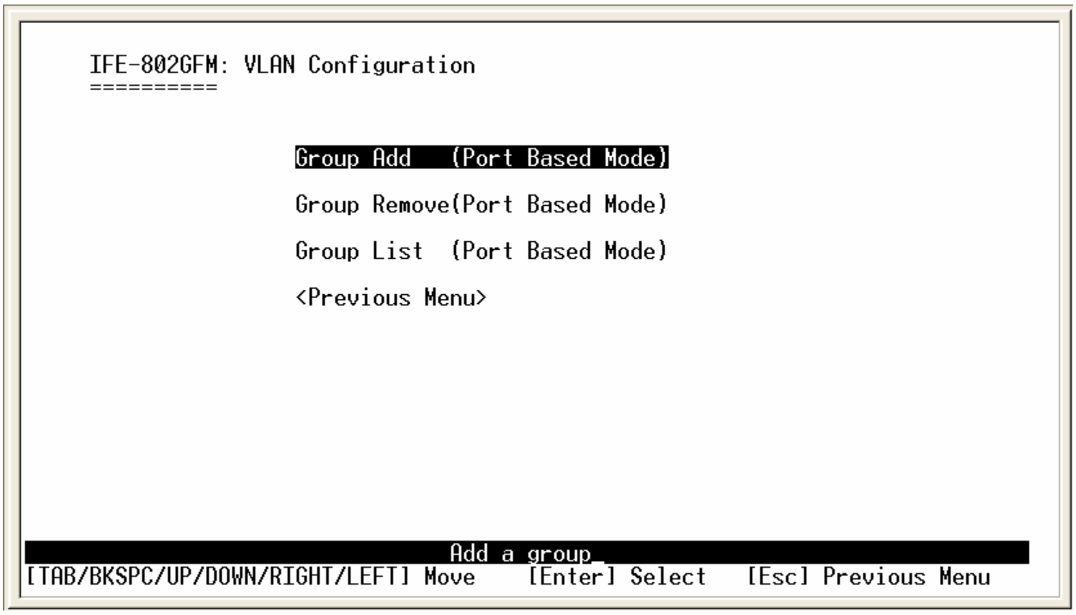


```
IFE-802GFM: VLAN Mode
==========

                VLAN Mode   :   Port Based










                                                                    [Apply]
                      Select the mode of VLAN.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

VLAN Mode Selection interface

Port Based VLAN Configuration

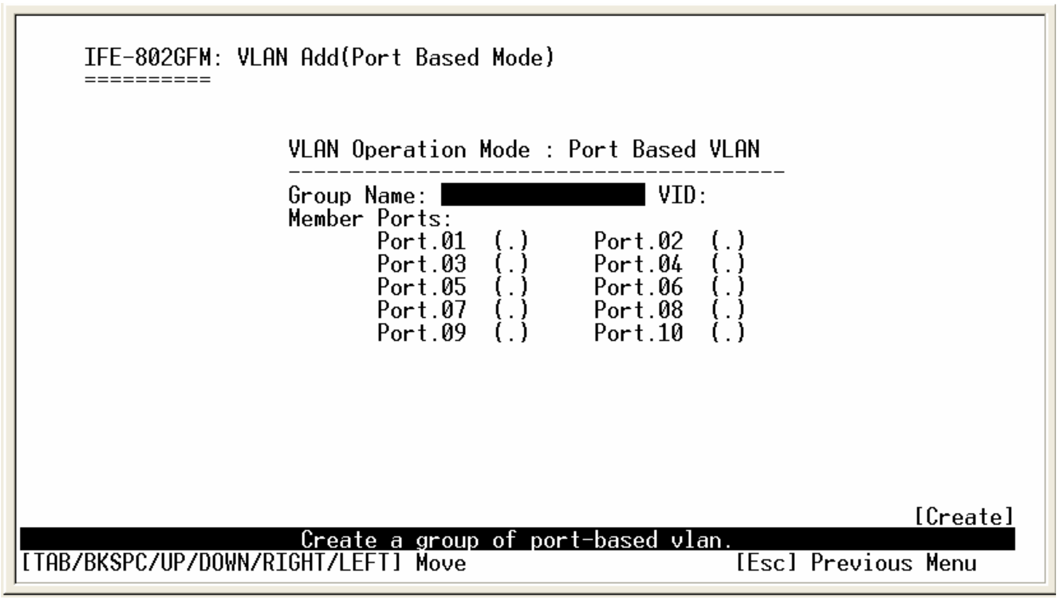
To add a VLAN group, remove a VLAN group, or view a VLAN group list, use the **Tab** key to move between the configuration items.



```
IFE-802GFM: VLAN Configuration
==========

                Group Add    (Port Based Mode)
                Group Remove(Port Based Mode)
                Group List  (Port Based Mode)
                <Previous Menu>

                                Add a group_
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Group Add

1. **Group Name:** Type a name for the new VLAN, ex: VLAN01.
2. **VID:** Type the VLAN group ID. The group ID range is from 1 to 4094.
   a. **Member Ports:** Press the ”**Space**” key to change the port status. Mark the port to be a member.
3. Select **<Create>** to save the configuration.
4. Press the **“ESC”** key to go back action menu line.

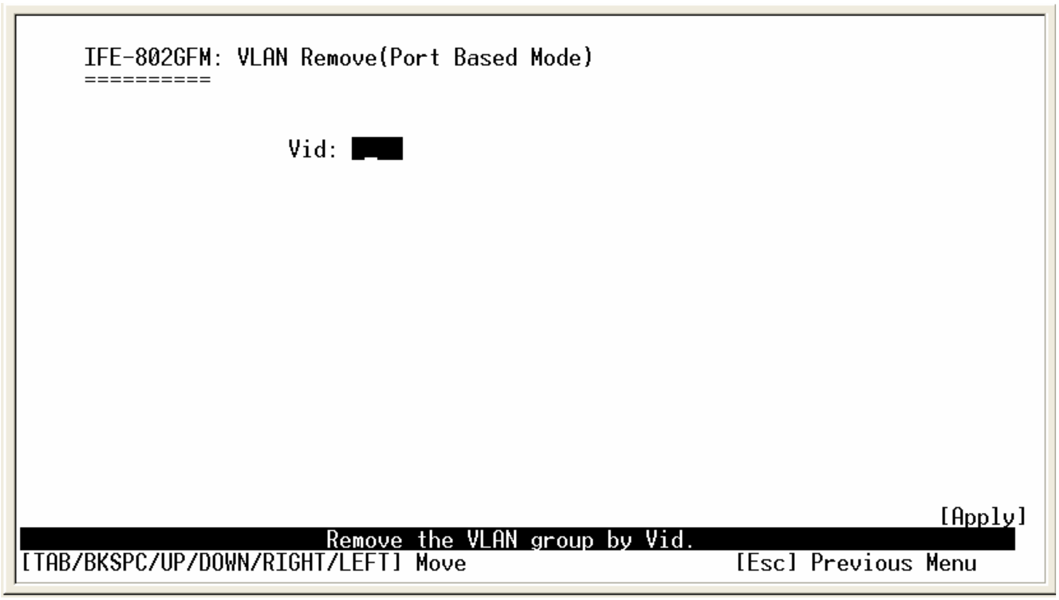


```
IFE-802GFM: VLAN Add(Port Based Mode)
==========

                VLAN Operation Mode : Port Based VLAN
                ---------------------------------------
                Group Name:                 VID:
                Member Ports:
                       Port.01  (.)     Port.02  (.)
                       Port.03  (.)     Port.04  (.)
                       Port.05  (.)     Port.06  (.)
                       Port.07  (.)     Port.08  (.)
                       Port.09  (.)     Port.10  (.)

                                                                [Create]
                      Create a group of port-based vlan.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                   [Esc] Previous Menu
```

Group Add interface

Removing a VLAN Group

You can remove an unwanted VLAN group. Enter the group Vid and select **<Apply>**.

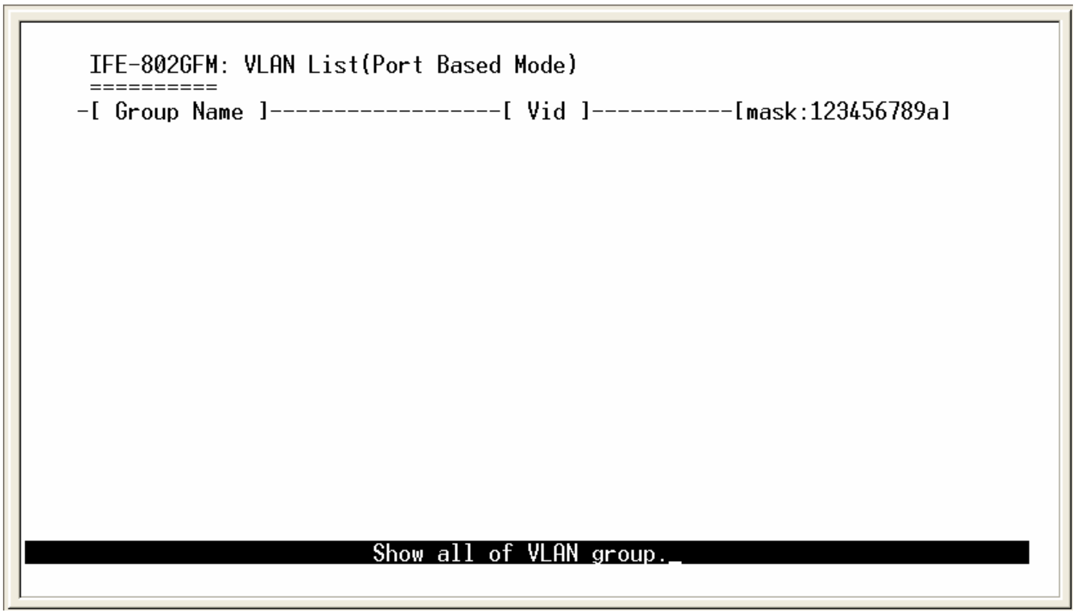


```
IFE-802GFM: VLAN Remove(Port Based Mode)
==========

                Vid:

                                                                  [Apply]
                        Remove the VLAN group by Vid.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                   [Esc] Previous Menu
```

Group Remove interface

Group List

Display all the VLAN group's information.

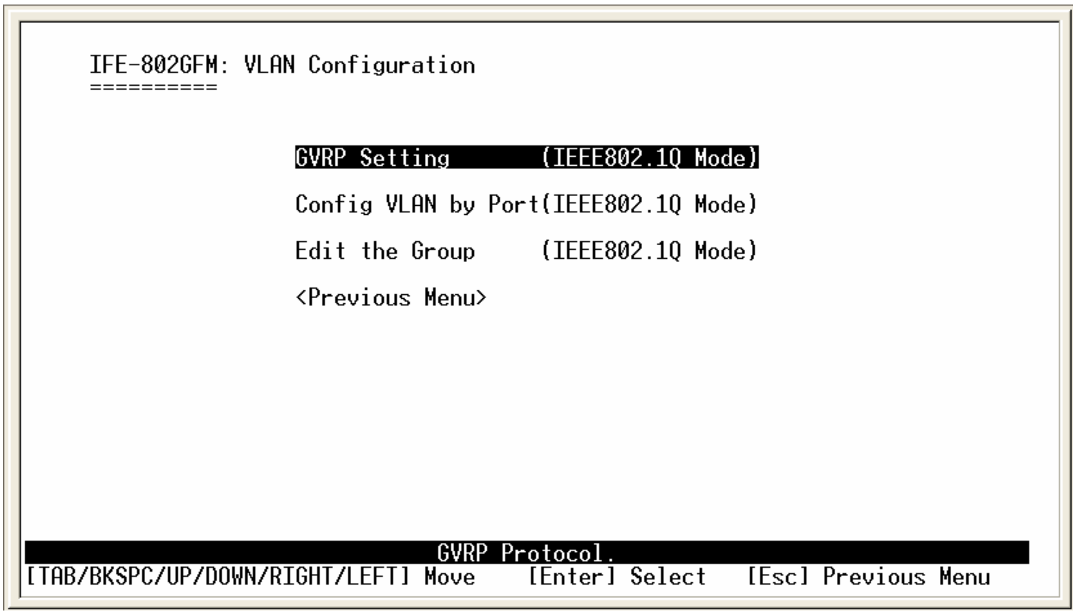


```
IFE-802GFM: VLAN List(Port Based Mode)
==========
-[ Group Name ]------------------[ Vid ]-----------[mask:123456789a]






                              Show all of VLAN group._
```

Group List interface

802.1Q VLAN Configuration

Configure GVRP setting, VLAN by port, and edit VLAN group.

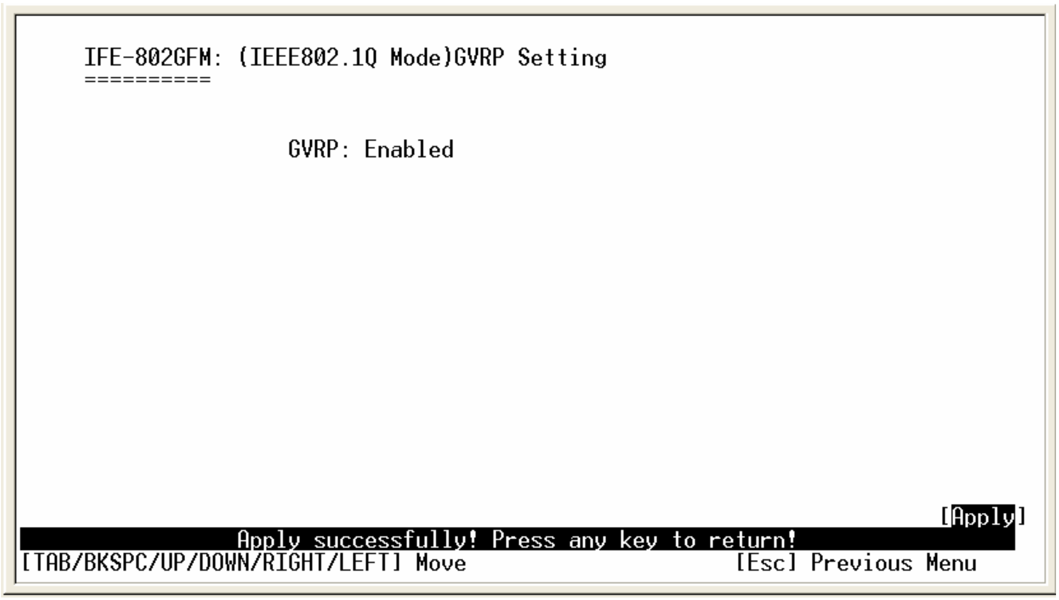


```
IFE-802GFM: VLAN Configuration
==========

                GVRP Setting       (IEEE802.1Q Mode)

                Config VLAN by Port(IEEE802.1Q Mode)

                Edit the Group     (IEEE802.1Q Mode)

                <Previous Menu>




                              GVRP Protocol.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

802.1Q VLAN Configuration interface

GVRP Setting

GVRP (Generic Attribute Registration Protocol) is an application defined in the IEEE 802.1Q standard that allows for the control of VLANs. Use the **Space** key to change the GVRP setting – Disable or Enable. Select the **Apply** to apply the setting.

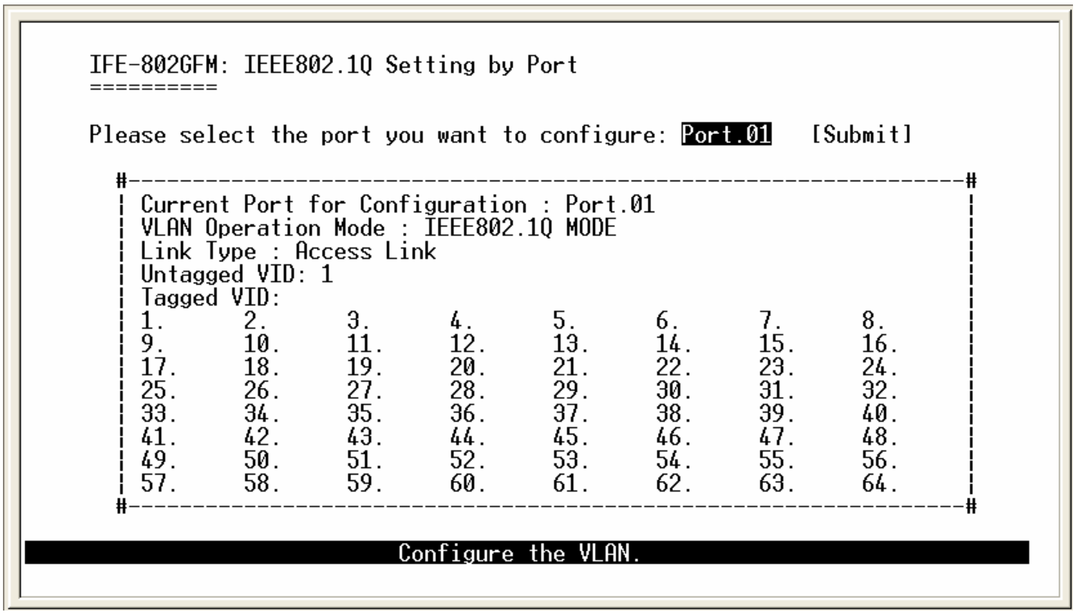


```
    IFE-802GFM: (IEEE802.1Q Mode)GVRP Setting
    ==========

                     GVRP: Enabled




                                                                   [Apply]
                  Apply successfully! Press any key to return!
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                       [Esc] Previous Menu
```

GVRP Setting interface

Configuring VLAN by Port

1. Select the port that you want to configure by using the **Spec** key. **Submit** to get the current port setting.
2. **Link Type**: There are 3 types.
   - **Access Link:** single switch only, allow the user to group ports by setting the same Vid.
   - **Trunk Link:** extended application of the **Access Link**, allows the user to group ports by setting the same Vid with 2 or more switches.
   - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
3. **Untagged Vid:** assign the untagged frame Vid.
4. **Tagged Vid:** assign the tagged frame Vid.
5. **Apply** the configuration.



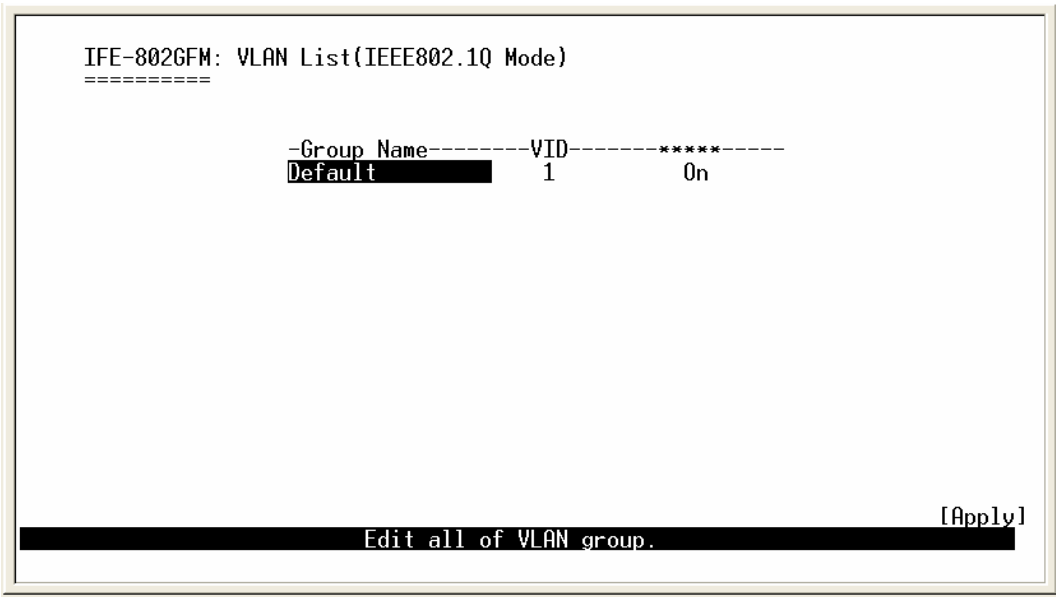
```
IFE-802GFM: IEEE802.1Q Setting by Port
==========

Please select the port you want to configure: Port.01   [Submit]

  #-----------------------------------------------------------------#
  | Current Port for Configuration : Port.01                        |
  | VLAN Operation Mode : IEEE802.1Q MODE                           |
  | Link Type : Access Link                                         |
  | Untagged VID: 1                                                 |
  | Tagged VID:                                                     |
  | 1.      2.      3.      4.      5.      6.      7.      8.      |
  | 9.      10.     11.     12.     13.     14.     15.     16.     |
  | 17.     18.     19.     20.     21.     22.     23.     24.     |
  | 25.     26.     27.     28.     29.     30.     31.     32.     |
  | 33.     34.     35.     36.     37.     38.     39.     40.     |
  | 41.     42.     43.     44.     45.     46.     47.     48.     |
  | 49.     50.     51.     52.     53.     54.     55.     56.     |
  | 57.     58.     59.     60.     61.     62.     63.     64.     |
  #-----------------------------------------------------------------#

                         Configure the VLAN.
```

Configuring the VLAN by Port interface

VLAN List

Enable or disable the VLAN group.

1. **Group Name:** you can rename the group name.
2. **On/Del:** On is the active VLAN group. Del removes the VLAN group.
3. After editing, press **<Apply>** to save the change.

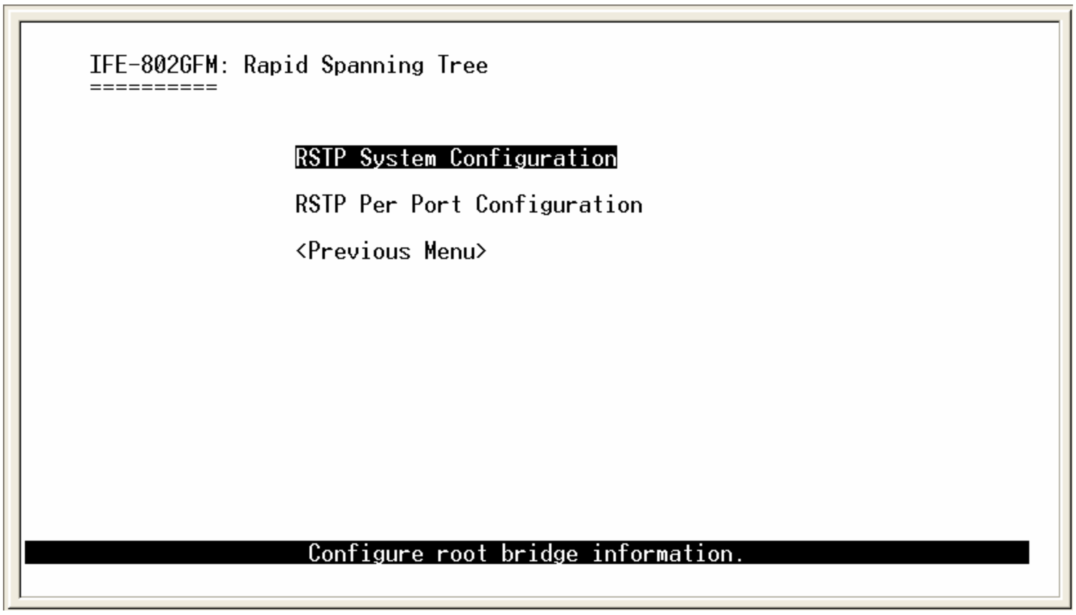


```
IFE-802GFM: VLAN List(IEEE802.1Q Mode)
==========

                   -Group Name--------VID-------*****-----
                   Default              1          On

                                                                    [Apply]
                         Edit all of VLAN group.
```

Edit VLAN Group interface

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.



```
IFE-802GFM: Rapid Spanning Tree
==========

                 RSTP System Configuration

                 RSTP Per Port Configuration

                 <Previous Menu>

                 Configure root bridge information.
```

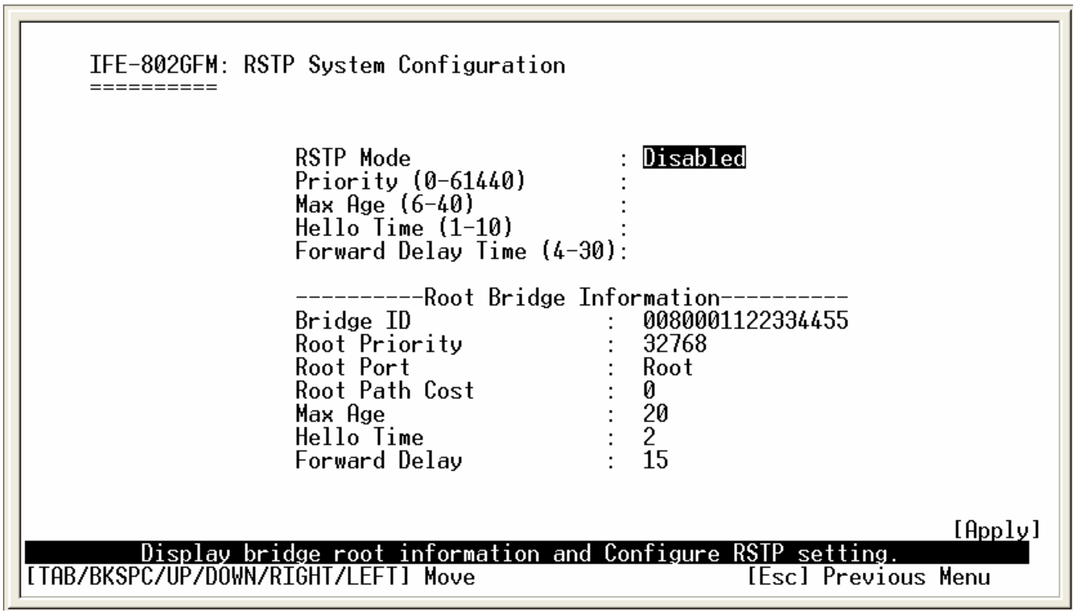
Rapid Spanning Tree interface

RSTP System Configuration

1. You can view the spanning tree information about the Root Bridge.
2. You can modify RSTP state. After modification, **Apply** the configuration.
   - **RSTP mode:** you must enable or disable the RSTP function before configuring the related parameters.
   - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If you change the value, you must reboot the switch to assign the path priority number. The value must be a multiple of 4096 according to the protocol standard rule.
   - **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
   - **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
   - **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.
3. Press **<Apply>** to save the configuration.

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)



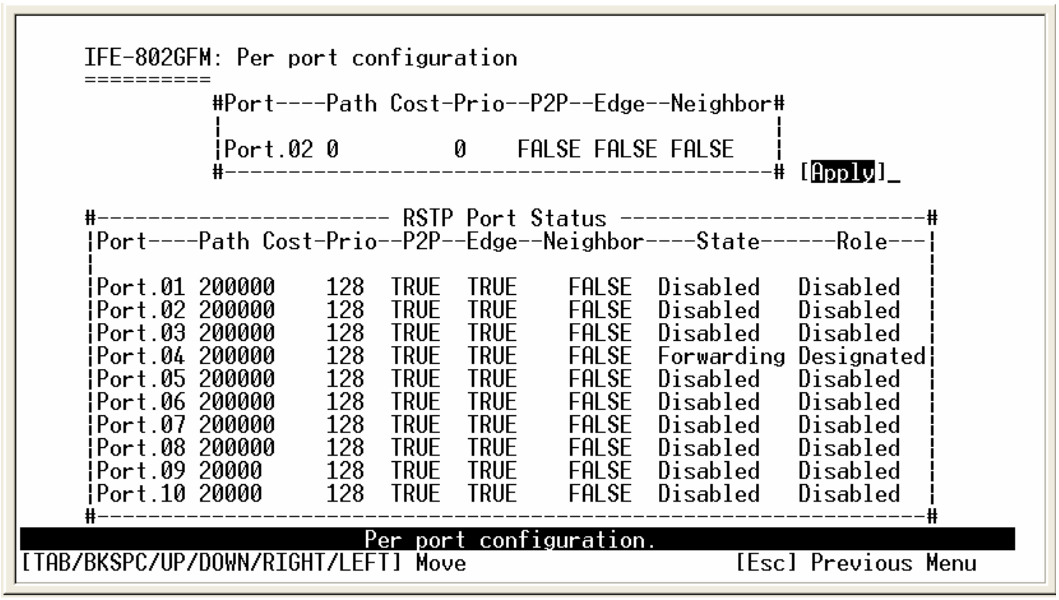
```
     IFE-802GFM: RSTP System Configuration
     ==========

                    RSTP Mode                : Disabled
                    Priority (0-61440)       :
                    Max Age (6-40)           :
                    Hello Time (1-10)        :
                    Forward Delay Time (4-30):

                    ----------Root Bridge Information----------
                    Bridge ID               :  0080001122334455
                    Root Priority           :  32768
                    Root Port               :  Root
                    Root Path Cost          :  0
                    Max Age                 :  20
                    Hello Time              :  2
                    Forward Delay           :  15


                                                                   [Apply]
         Display bridge root information and Configure RSTP setting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                     [Esc] Previous Menu
```

RSTP System Configuration interface

RSTP Port Configuration

You can configure the path cost and priority of every port.

1. Select the port in the Port column.
2. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
3. **Priority:** Decide which port should be blocked by priority in the LAN. Enter a number 0 through 240. The value of the priority must be a multiple of 16.
4. **P2P:** Some of the rapid state transactions that might be possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
5. **Edge:** The port directly connected to end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
6. **Neighbor:** The port includes the STP mathematic calculation. **True** is not including the STP mathematic calculation. **False** is including the STP mathematic calculation.
7. **Apply** the setting.

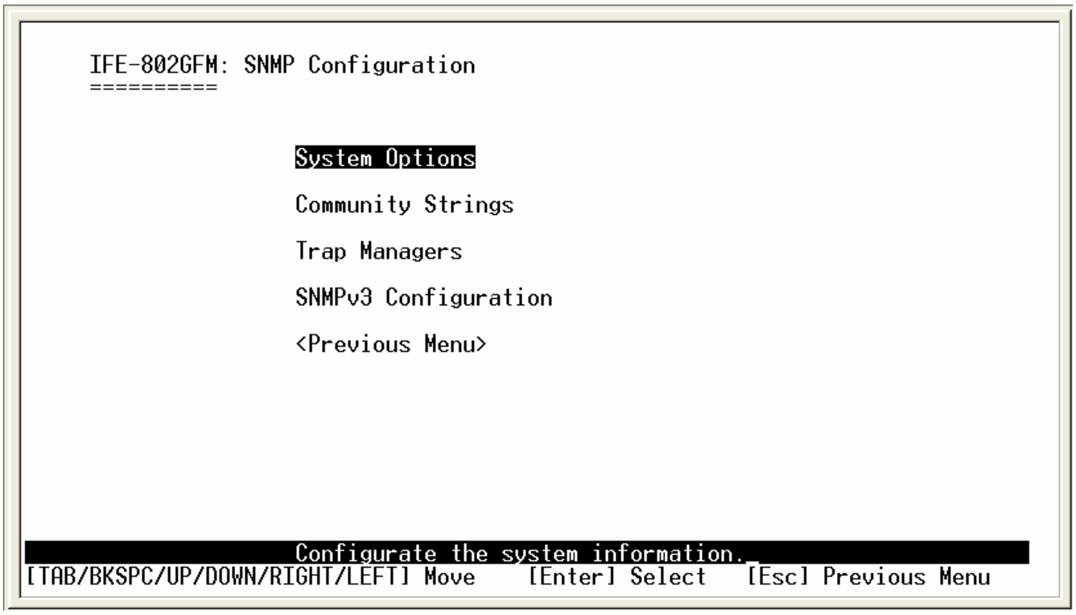


```
     IFE-802GFM: Per port configuration
     ==========
               #Port----Path Cost-Prio--P2P--Edge--Neighbor#
               |                                           |
               |Port.02 0         0    FALSE FALSE FALSE   |
               #-------------------------------------------# [Apply]_

     #----------------------- RSTP Port Status ------------------------#
     |Port----Path Cost-Prio--P2P--Edge--Neighbor----State------Role---|
     |                                                                  |
     |Port.01 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.02 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.03 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.04 200000    128  TRUE  TRUE    FALSE  Forwarding Designated|
     |Port.05 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.06 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.07 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.08 200000    128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.09 20000     128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     |Port.10 20000     128  TRUE  TRUE    FALSE  Disabled   Disabled  |
     #-----------------------------------------------------------------#
                           Per port configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                 [Esc] Previous Menu
```

RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.



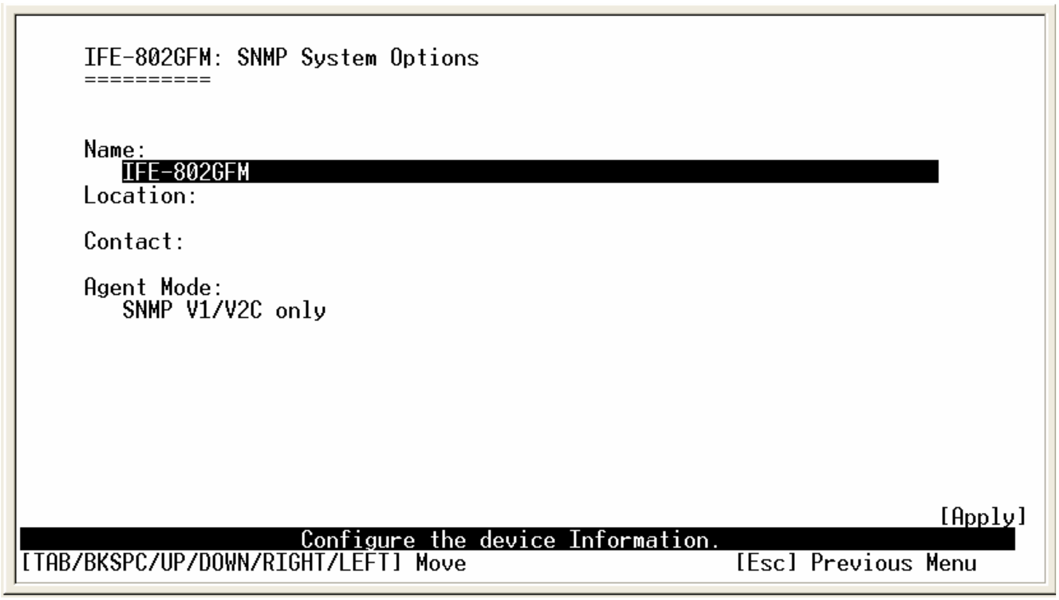
```
IFE-802GFM: SNMP Configuration
==========

                System Options

                Community Strings

                Trap Managers

                SNMPv3 Configuration

                <Previous Menu>

                    Configurate the system information._
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

SNMP Configuration interface

System Options

Enter the system name, contact, and location information.

1. **Name:** assign a name for the switch.
2. **Contact:** Type the name of contact person or organization.
3. **Location:** Type the location of the switch.
4. **Agent Mode:** Select the SNMP version that you want to use.
5. **<Apply>** to save configure value.



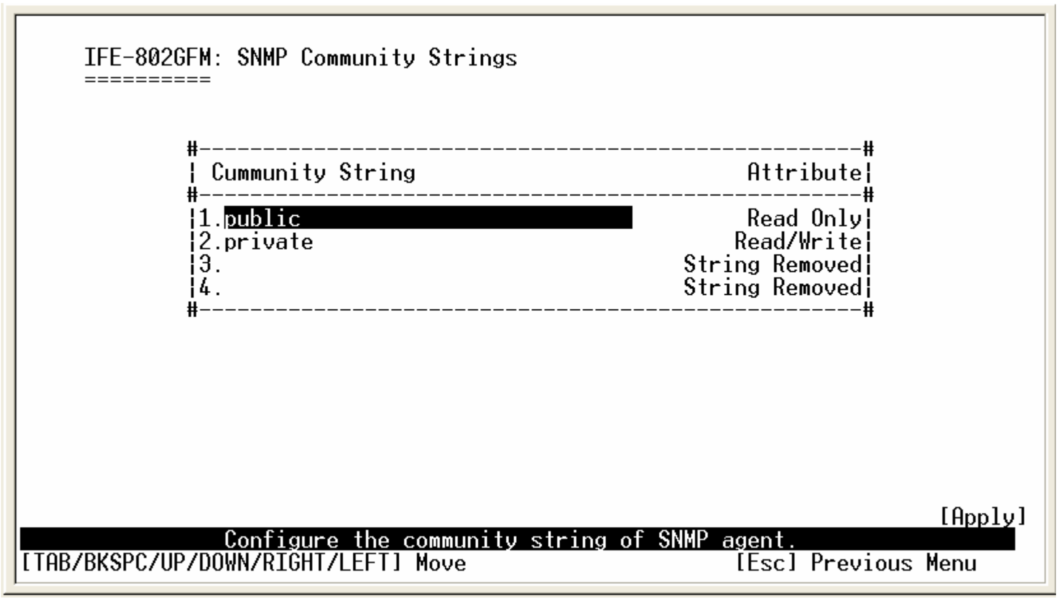
```
IFE-802GFM: SNMP System Options
==========

Name:
   IFE-802GFM
Location:

Contact:

Agent Mode:
   SNMP V1/V2C only

                                                                  [Apply]
                    Configure the device Information.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

SNMP System Options interface

Community Strings

You can change the default community string, public and private attribute, and define two more set community string.

1. **Community Name:** It uses for authenticating the manager to allow access the agent. Type the name of community strings. The Public and Private Community string cannot be changed the name.
2. **Attribute:** enable the access rights is read only or read/write or string removed.
   - **Read only:** Read only, enables requests accompanied by this string to display MIB-object information.
   - **Read/Write:** Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.
   - **String Removed:** this community string is disabling.
3. **Apply** the configuration.



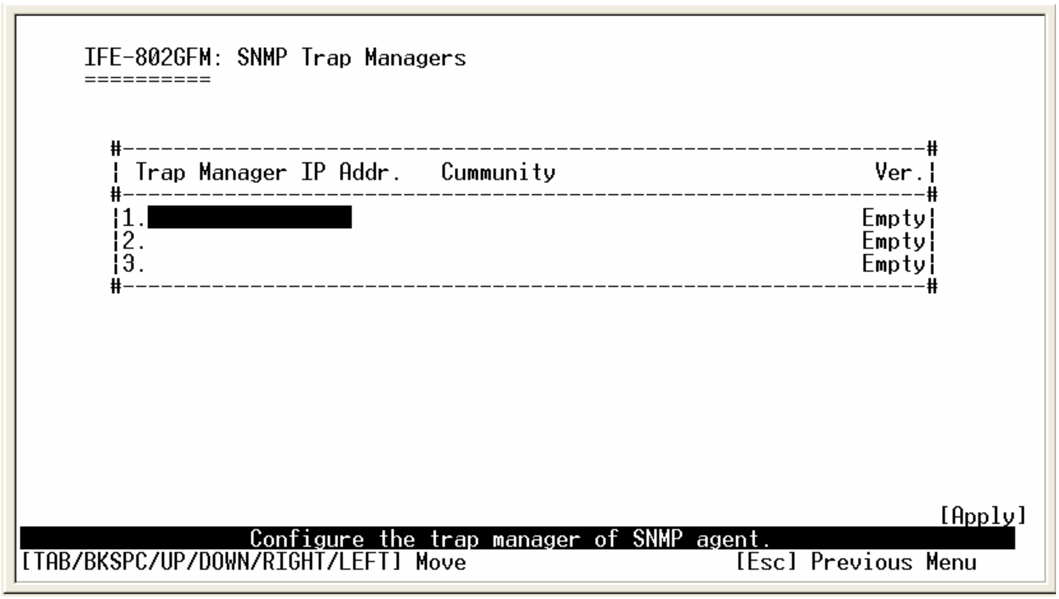
```
    IFE-802GFM: SNMP Community Strings
    ==========

              #-----------------------------------------------------#
              | Cummunity String                           Attribute|
              #-----------------------------------------------------#
              |1.public                                   Read Only|
              |2.private                                 Read/Write|
              |3.                                    String Removed|
              |4.                                    String Removed|
              #-----------------------------------------------------#






                                                                      [Apply]
                     Configure the community string of SNMP agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                        [Esc] Previous Menu
```

Add Community Strings interface

Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

1. **Trap Manager IP:** enter the IP address of the trap manager.
2. **Community Name:** enter the community string.
3. **Ver.:** select the SNMP version type – v1 or v2.
4. **<Apply>** to save the configuration
5. To disable the trap manager, please delete the trap manager IP, community string and version. And then, save the change.

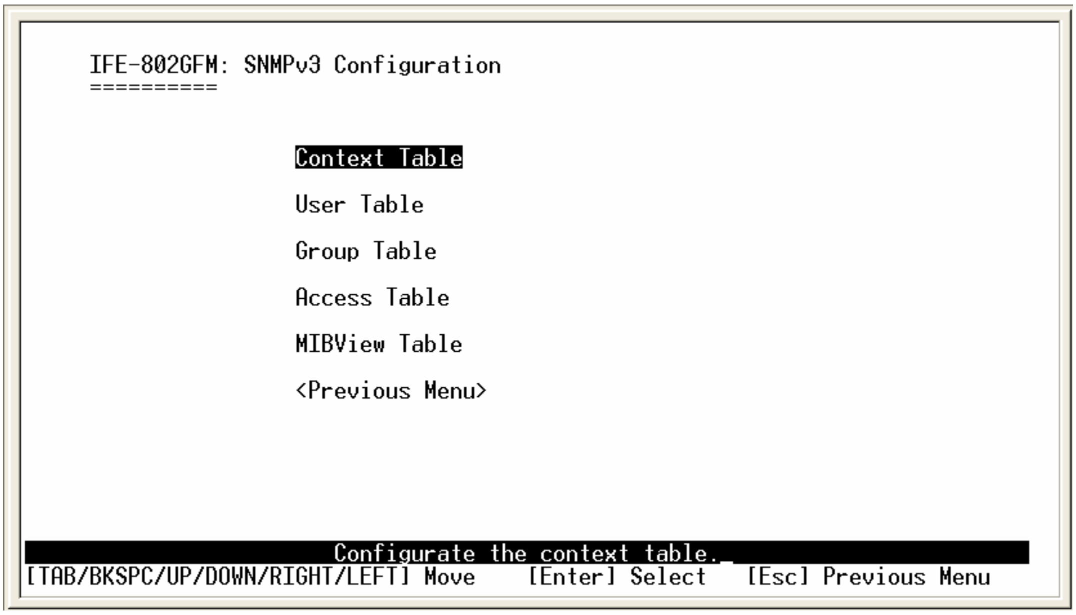


```
    IFE-802GFM: SNMP Trap Managers
    ==========

      #----------------------------------------------------------------#
      | Trap Manager IP Addr.   Cummunity                         Ver.|
      #----------------------------------------------------------------#
      |1.                                                        Empty|
      |2.                                                        Empty|
      |3.                                                        Empty|
      #----------------------------------------------------------------#

                                                                    [Apply]
                       Configure the trap manager of SNMP agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                       [Esc] Previous Menu
```

Trap Managers interface

SNMP v3 Configuration

Configure the SNMP v3 function.

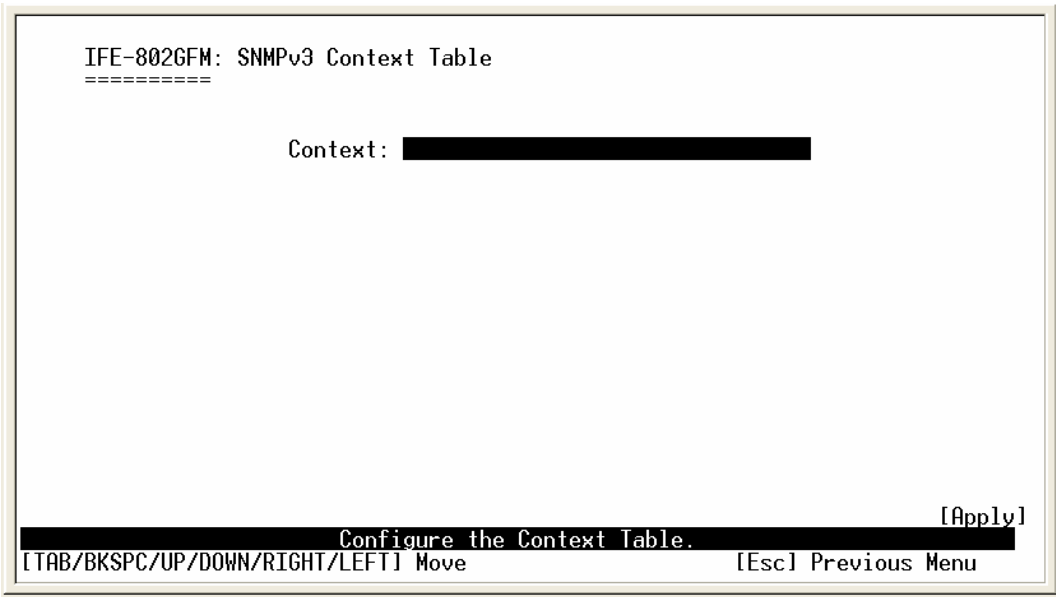


```
IFE-802GFM: SNMPv3 Configuration
==========

                Context Table
                User Table
                Group Table
                Access Table
                MIBView Table
                <Previous Menu>

                    Configurate the context table._
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

SNMP v3 configuration interface

Context Table

Configuring the SNMP v3 context table. Assign the context name in the context table.



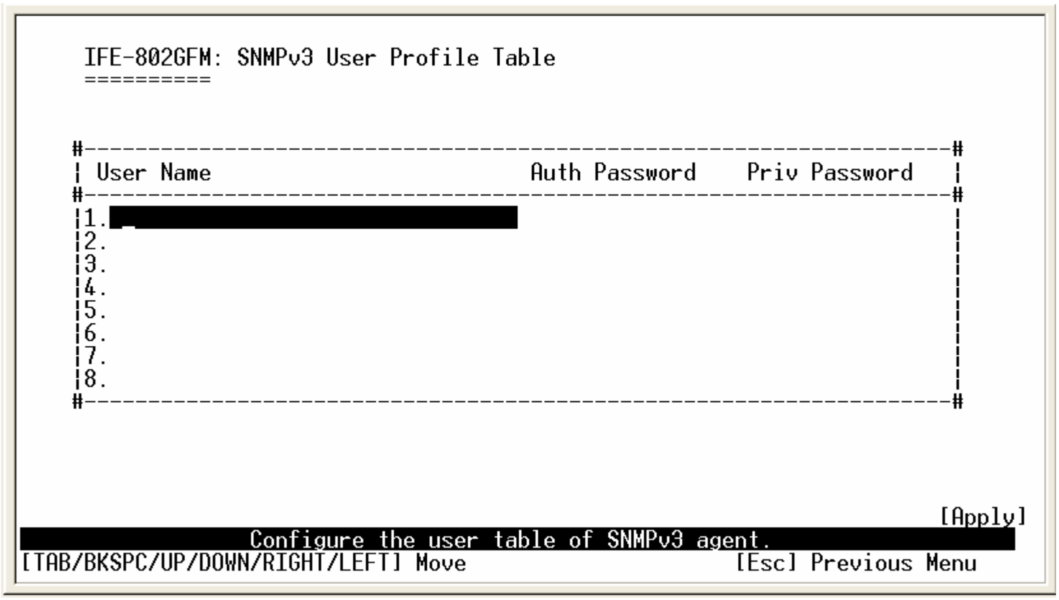
```
IFE-802GFM: SNMPv3 Context Table
==========

                Context:

                                                              [Apply]
                      Configure the Context Table.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

SNMP v3 Context Table interface

User Table

Configure SNMP v3 user table..

1. **User Name:** set up the user name.
2. **Auth Password:** set up the authentication password.
3. **Priv Password:** set up the private password.
4. **<Apply>** to save the configuration



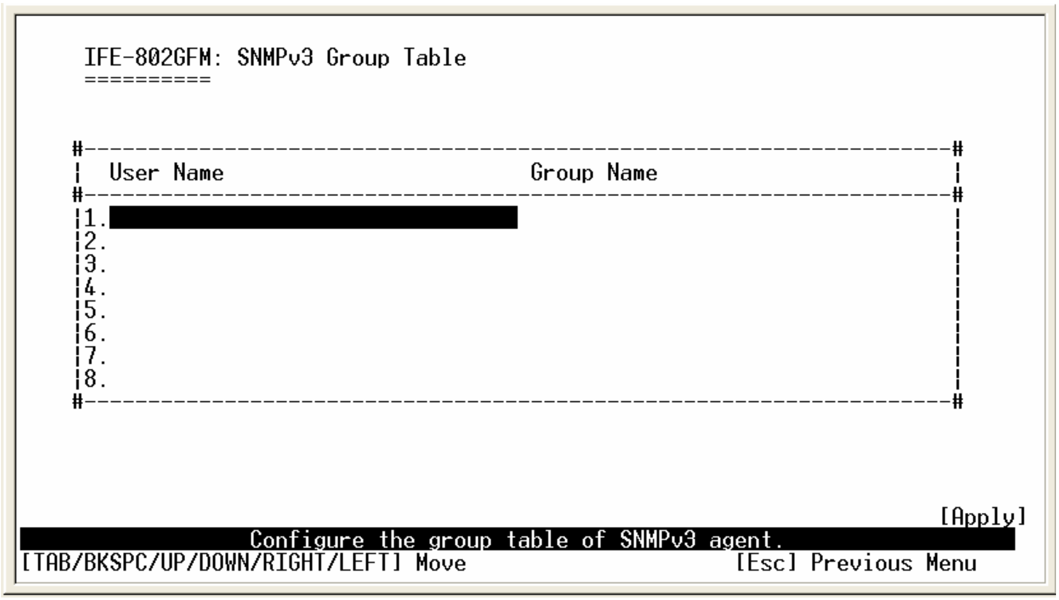
```
      IFE-802GFM: SNMPv3 User Profile Table
      ==========


     #-------------------------------------------------------------------#
     | User Name                         Auth Password    Priv Password   |
     #-------------------------------------------------------------------#
     |1.                                                                  |
     |2.                                                                  |
     |3.                                                                  |
     |4.                                                                  |
     |5.                                                                  |
     |6.                                                                  |
     |7.                                                                  |
     |8.                                                                  |
     #-------------------------------------------------------------------#




                                                                      [Apply]
                  Configure the user table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

SNMP v3 User Profile Table interface

Group Table

Configure SNMP v3 group table.

1. **User Name:** assign the user name that you have set up in user table.
2. **Group Name:** set up the group name.
3. **<Apply>** to save the configuration

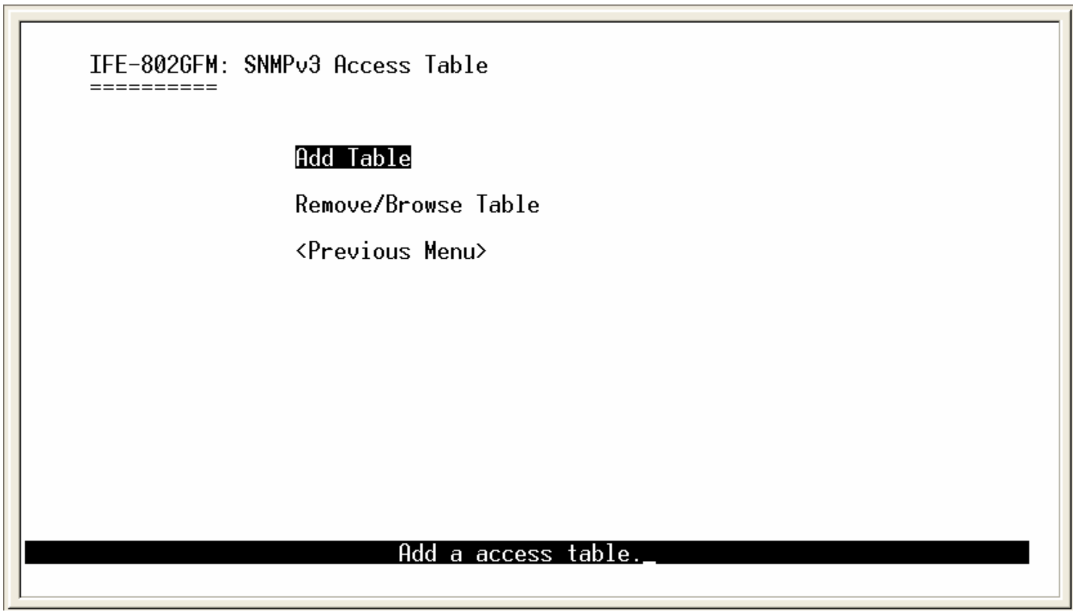


```
    IFE-802GFM: SNMPv3 Group Table
    ==========


   #----------------------------------------------------------------------#
   |  User Name                        Group Name                         |
   #----------------------------------------------------------------------#
   |1.                                                                    |
   |2.                                                                    |
   |3.                                                                    |
   |4.                                                                    |
   |5.                                                                    |
   |6.                                                                    |
   |7.                                                                    |
   |8.                                                                    |
   #----------------------------------------------------------------------#




                                                                    [Apply]
                  Configure the group table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                        [Esc] Previous Menu
```

SNMP v3 Group Table interface

Access Table

Configuring the SNMP v3 access table.



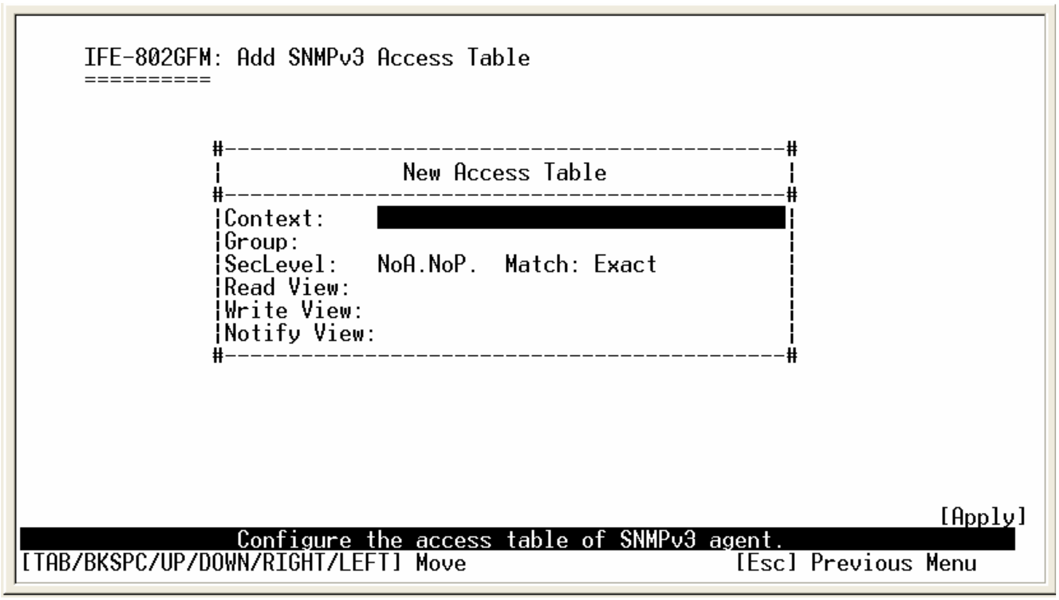
```
    IFE-802GFM: SNMPv3 Access Table
    ==========

                    Add Table

                    Remove/Browse Table

                    <Previous Menu>











                             Add a access table._
```

SNMP v3 AccessTable interface

■ Add Table

Add the access table.

1. **Context:** set up the context name.
2. **Group:** set up the group.
3. **Sec Level:** select the access level.
4. **Read View:** set up the read view.
5. **Write View:** set up the write view.
6. **Notify View:** Set up the notify view.
7. **<Apply>** to save all configurations.

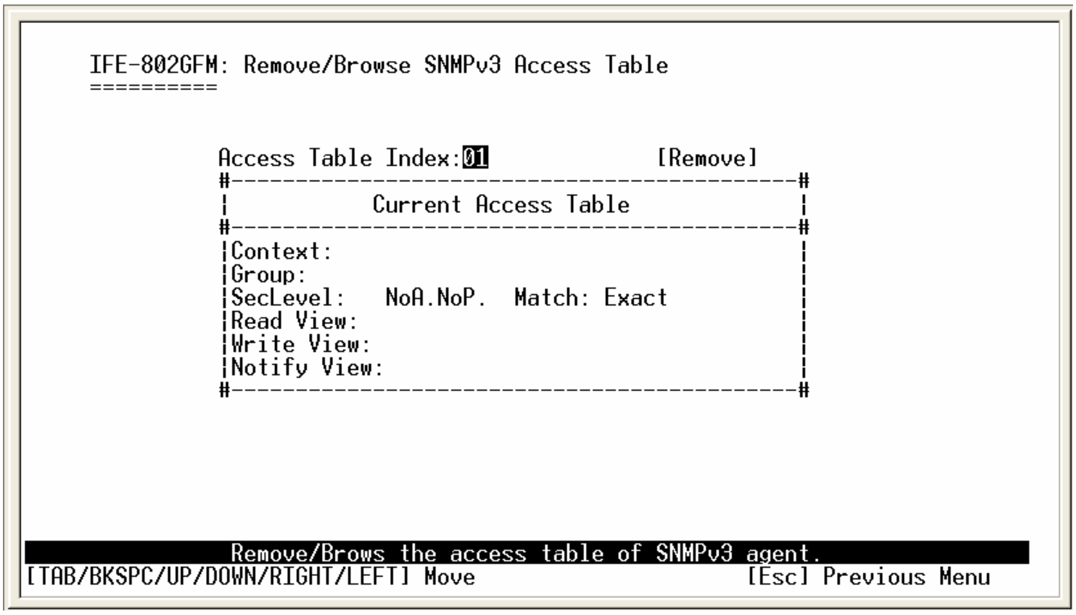


```
     IFE-802GFM: Add SNMPv3 Access Table
     ==========


               #--------------------------------------------#
               |              New Access Table              |
               #--------------------------------------------#
               |Context:                                    |
               |Group:                                      |
               |SecLevel:    NoA.NoP.  Match: Exact         |
               |Read View:                                  |
               |Write View:                                 |
               |Notify View:                                |
               #--------------------------------------------#




                                                        [Apply]
                 Configure the access table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move              [Esc] Previous Menu
```

- **Remove/Browse Table**

Remove and Browse access table.

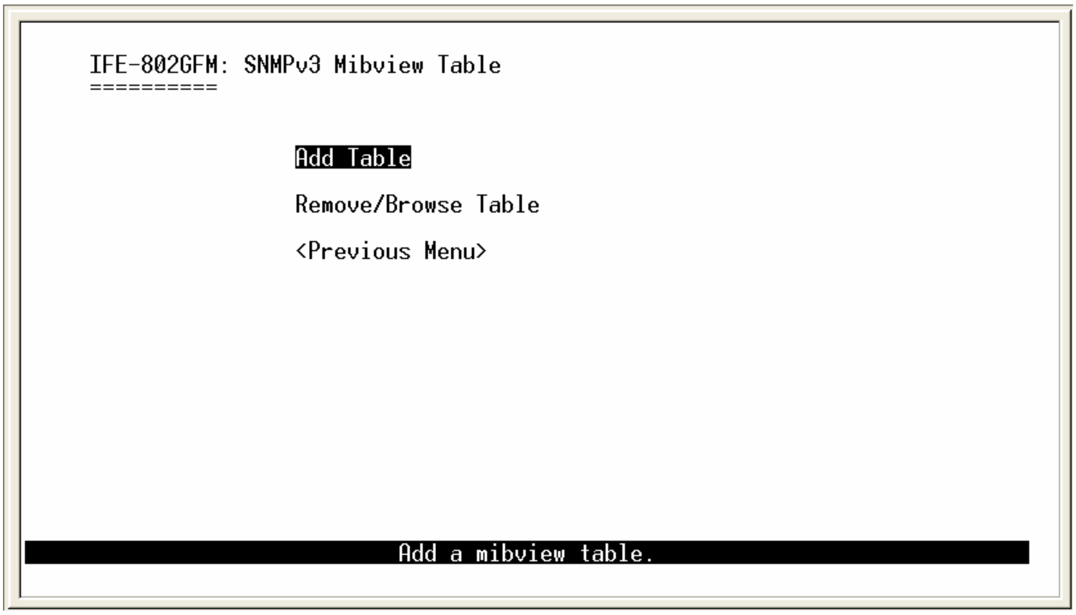
1. **Access Table Index:** press the **space** key to select the Access Table Index which is to be removed.
2. **Remove:** be sure of the selected index and press the **enter** key to remove
3. **Context:** display the context information**..**
4. **Group:** display the group information.
5. **SecLevel:** display the SecLevel information.
6. **Read View:** display the Read View information.
7. **Write View:** display the Write View information.
8. **Notify View:** display the Notify View information.



```
IFE-802GFM: Remove/Browse SNMPv3 Access Table
==========

          Access Table Index:01            [Remove]
          #---------------------------------------------#
          |            Current Access Table             |
          #---------------------------------------------#
          |Context:                                     |
          |Group:                                       |
          |SecLevel:   NoA.NoP.  Match: Exact           |
          |Read View:                                   |
          |Write View:                                  |
          |Notify View:                                 |
          #---------------------------------------------#

                Remove/Brows the access table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                  [Esc] Previous Menu
```

MIBview Table

Configuring the MIB view table.



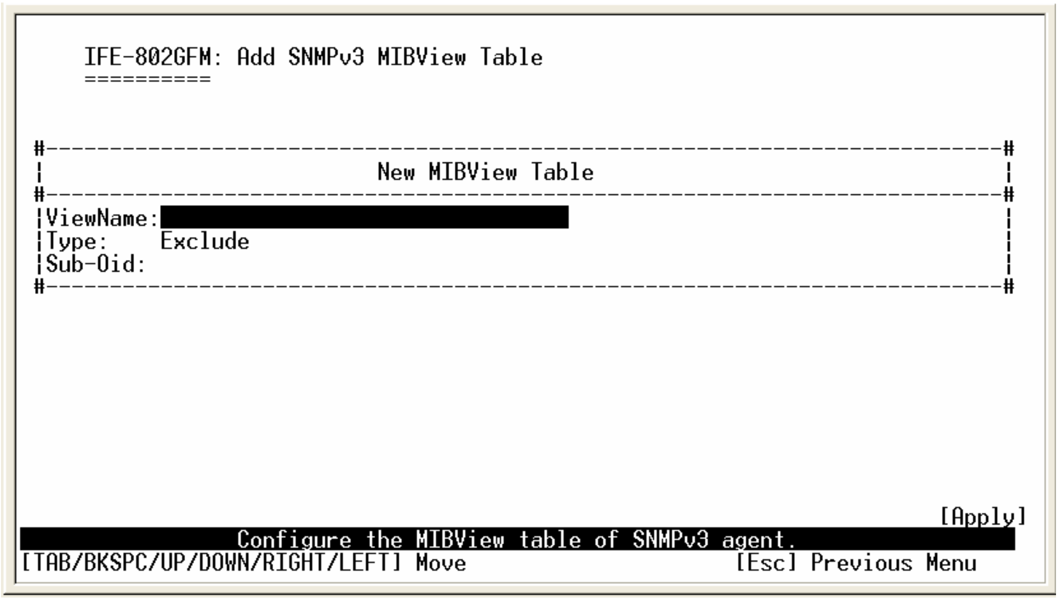
```
IFE-802GFM: SNMPv3 Mibview Table
==========

                Add Table

                Remove/Browse Table

                <Previous Menu>

                             Add a mibview table.
```

SNMP v3 MIBviewTable interface

- **Add Table**

Add a MIB view table.

1. **ViewName:** set up the name.
2. **Type:** select the type – exclude or include.
3. **Sub-Oid:** fill the Sub OID.
4. **<Apply>** to save the configuration

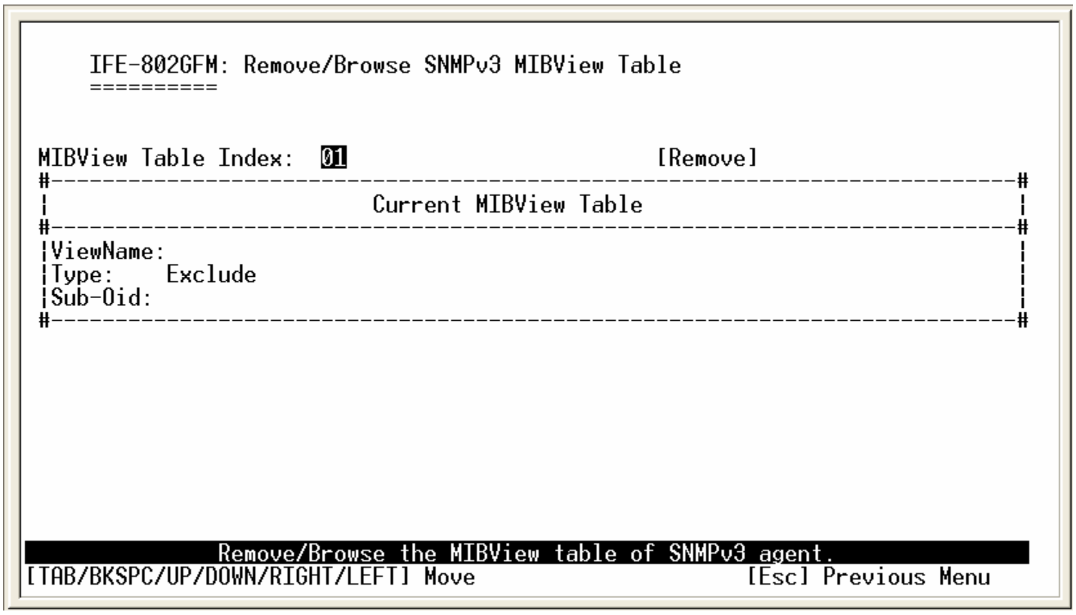


```
    IFE-802GFM: Add SNMPv3 MIBView Table
    ==========

#--------------------------------------------------------------------------#
|                              New MIBView Table                           |
#--------------------------------------------------------------------------#
|ViewName:                                                                 |
|Type:     Exclude                                                         |
|Sub-Oid:                                                                  |
#--------------------------------------------------------------------------#

                                                                    [Apply]
                  Configure the MIBView table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

- **Remove/Browse Table**

Remove and Browse MIBview table.

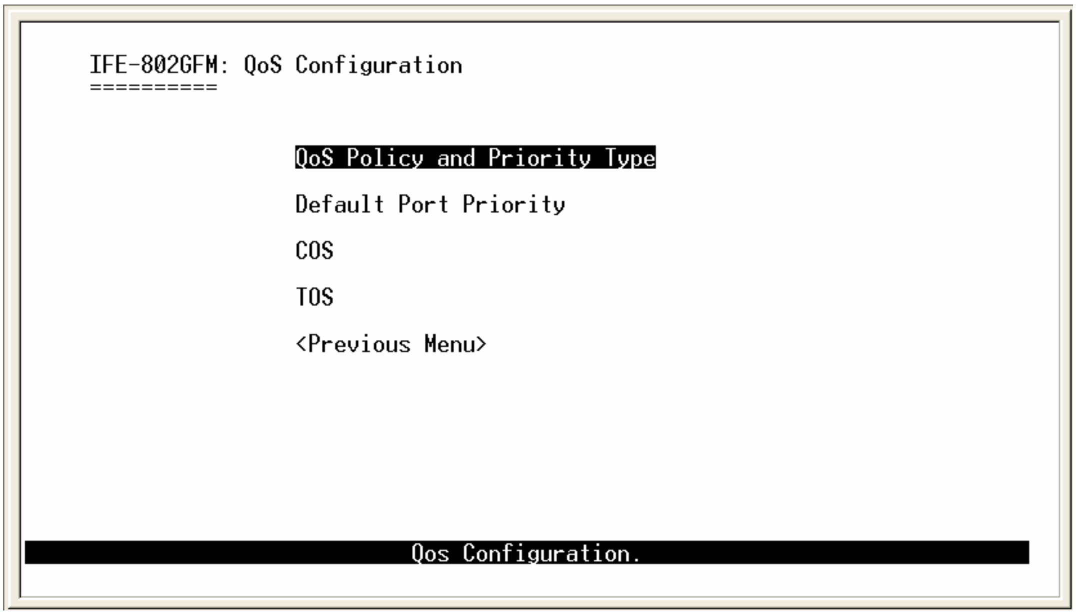
1. **MIBView Table Index**: press the **space** key to select the **MIBView Table Index** which is to be removed.
2. **Remove**: be sure of the selected index and press the **enter** key to remove.
3. **ViewName**: display the information of ViewName.
4. **Type**: display the type of information.
5. **Sub-Oid:** display the information of Sub-Oid.



```
     IFE-802GFM: Remove/Browse SNMPv3 MIBView Table
     ==========

 MIBView Table Index:  01                        [Remove]
 #-----------------------------------------------------------------------------#
 |                          Current MIBView Table                              |
 #-----------------------------------------------------------------------------#
 |ViewName:                                                                    |
 |Type:    Exclude                                                             |
 |Sub-Oid:                                                                     |
 #-----------------------------------------------------------------------------#







                Remove/Browse the MIBView table of SNMPv3 agent.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                       [Esc] Previous Menu
```

QoS Configuration

You can configure the Qos policy and priority settings, port priority settings, COS and TOS settings.

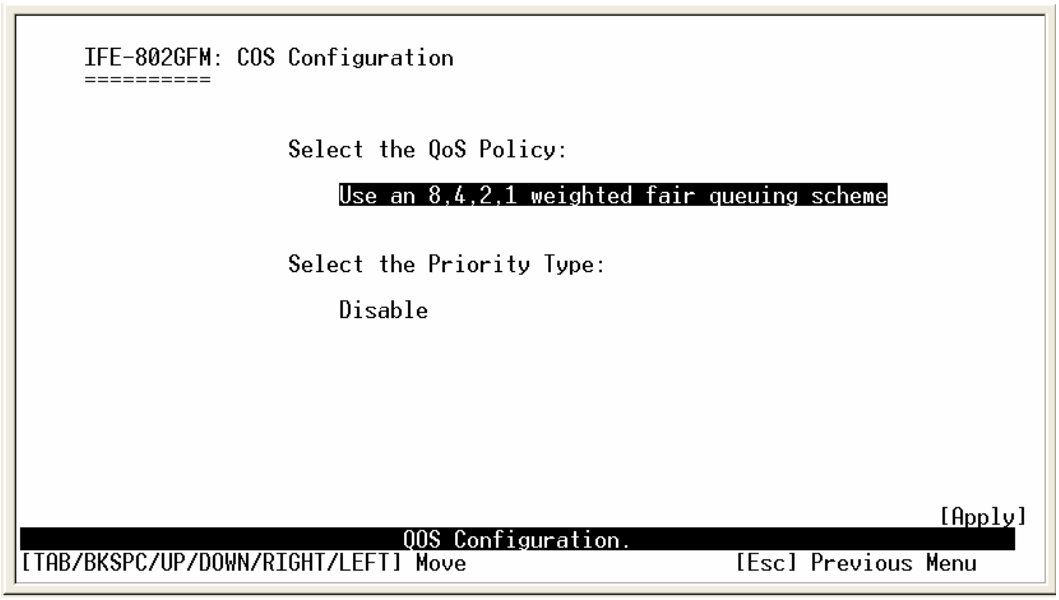


```
     IFE-802GFM: QoS Configuration
     ==========

                     QoS Policy and Priority Type

                     Default Port Priority

                     COS

                     TOS

                     <Previous Menu>






                                Qos Configuration.
```

QoS Configuration interface

QoS Policy and Priority Type

- **Select the Qos Policy:** Select the Qos policy rule
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rating to process the priority queue from High to Lowest queue. For example: the system will process 80 % high queue traffic, 40 % middle queue traffic, 20 % low queue traffic, and 10 % lowest queue traffic at the same time. And the traffic in the Low Priority queue is not transmitted until all High, Medium, and Normal traffic are serviced.
  - **Use the strict priority scheme:** The higher queue will always be processed first, except when the higher queue is empty
- **Select the Priority Type:** Every port has 5 priority type selections. Disable means no priority type is selected
  - **Port-base:** The port priority will follow the **default port priority** that has been assigned – High, middle, low, or lowest
  - **COS only:** The port priority will only follow the **COS priority** that has been assigned
  - **TOS only:** The port priority will only follow the **TOS priority** that has been assigned
  - **COS first:** The port priority will follow the COS priority first, and then other priority rule
  - **TOS first:** The port priority will follow the TOS priority first, and the other priority rule
- Select the **<Apply>** to save the configuration



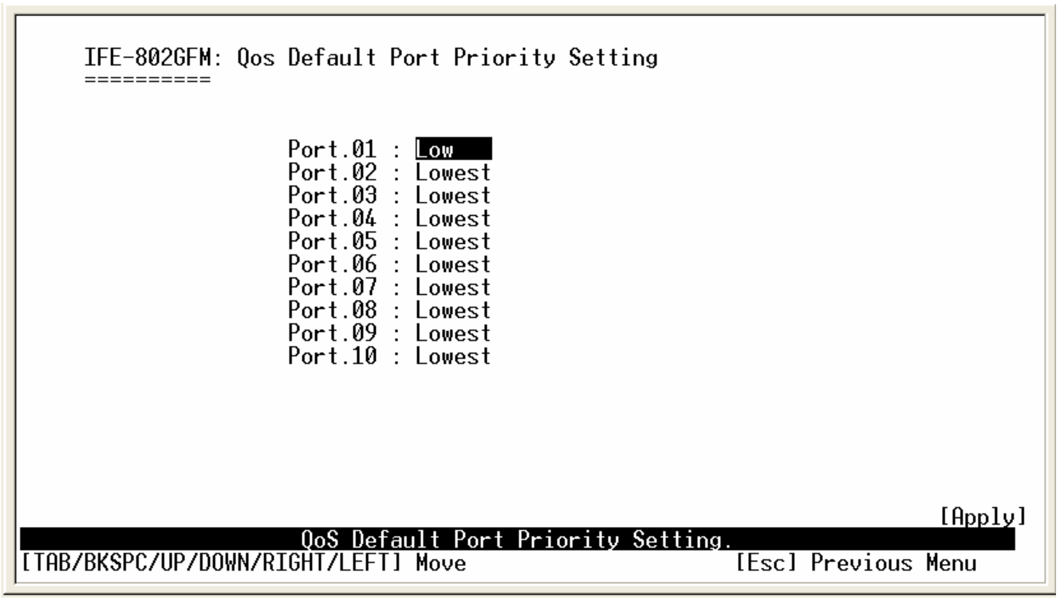
```
IFE-802GFM: COS Configuration
==========

                    Select the QoS Policy:

                         Use an 8,4,2,1 weighted fair queuing scheme

                    Select the Priority Type:

                         Disable




                                                                    [Apply]
                                     QOS Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                       [Esc] Previous Menu
```

QoS Policy and Priority Type interface

Default Port Priority

Configure the port priority level.

- **Port 1 ~ 10:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- **Apply** the configuration.



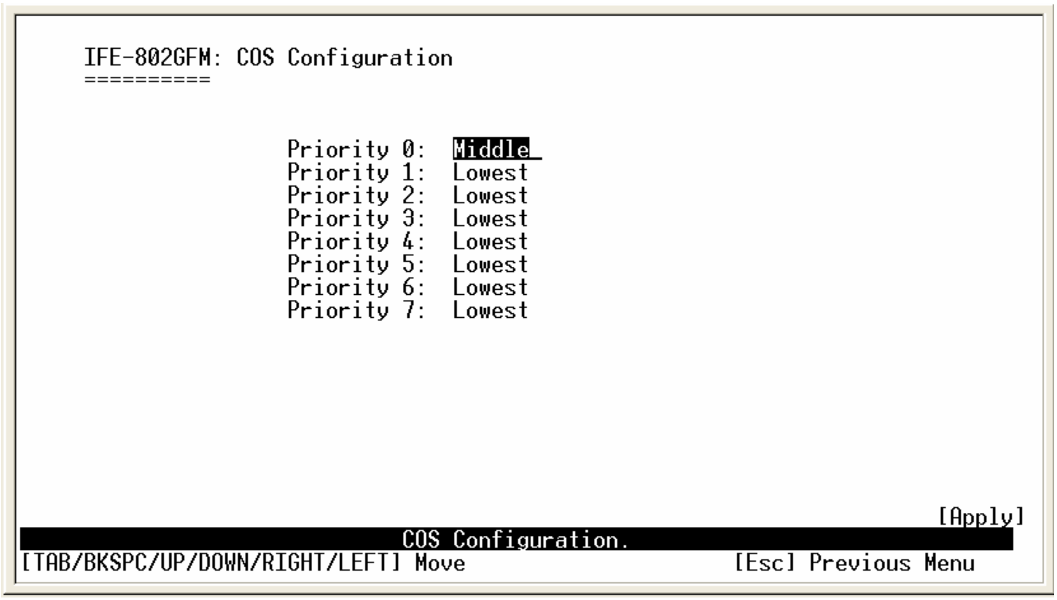
```
IFE-802GFM: Qos Default Port Priority Setting
==========

                    Port.01 : Low
                    Port.02 : Lowest
                    Port.03 : Lowest
                    Port.04 : Lowest
                    Port.05 : Lowest
                    Port.06 : Lowest
                    Port.07 : Lowest
                    Port.08 : Lowest
                    Port.09 : Lowest
                    Port.10 : Lowest



                                                                    [Apply]
                           QoS Default Port Priority Setting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                       [Esc] Previous Menu
```

Default Port Priority Setting interface

COS Configuration

Set up the COS priority level.

- **COS priority:**. Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- **Apply** the configuration.



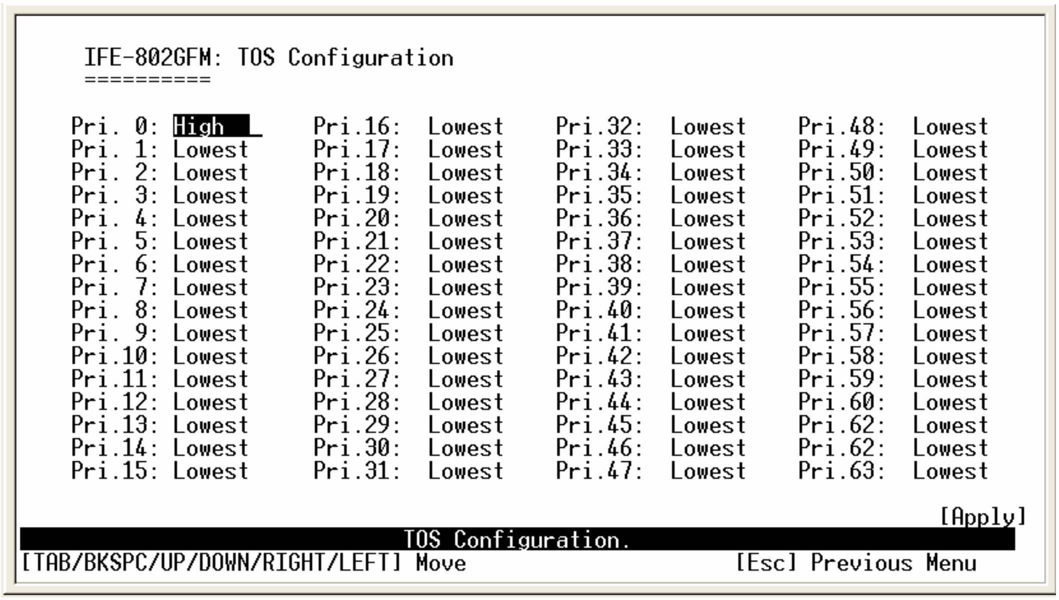
```
     IFE-802GFM: COS Configuration
     ==========

                    Priority 0:  Middle
                    Priority 1:  Lowest
                    Priority 2:  Lowest
                    Priority 3:  Lowest
                    Priority 4:  Lowest
                    Priority 5:  Lowest
                    Priority 6:  Lowest
                    Priority 7:  Lowest



                                                                      [Apply]
                                 COS Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                     [Esc] Previous Menu
```

COS Configuration interface

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority levels. Each level has 4 types of priority – high, middle, low, and lowest. The default value is the “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example: the user sets the TOS to level 25 (high). The port 1 is following the TOS priority policy only. When the port 1 packet is received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- **Apply** the configuration.



```
IFE-802GFM: TOS Configuration
==========

Pri. 0: High        Pri.16:  Lowest    Pri.32:  Lowest    Pri.48:  Lowest
Pri. 1: Lowest      Pri.17:  Lowest    Pri.33:  Lowest    Pri.49:  Lowest
Pri. 2: Lowest      Pri.18:  Lowest    Pri.34:  Lowest    Pri.50:  Lowest
Pri. 3: Lowest      Pri.19:  Lowest    Pri.35:  Lowest    Pri.51:  Lowest
Pri. 4: Lowest      Pri.20:  Lowest    Pri.36:  Lowest    Pri.52:  Lowest
Pri. 5: Lowest      Pri.21:  Lowest    Pri.37:  Lowest    Pri.53:  Lowest
Pri. 6: Lowest      Pri.22:  Lowest    Pri.38:  Lowest    Pri.54:  Lowest
Pri. 7: Lowest      Pri.23:  Lowest    Pri.39:  Lowest    Pri.55:  Lowest
Pri. 8: Lowest      Pri.24:  Lowest    Pri.40:  Lowest    Pri.56:  Lowest
Pri. 9: Lowest      Pri.25:  Lowest    Pri.41:  Lowest    Pri.57:  Lowest
Pri.10: Lowest      Pri.26:  Lowest    Pri.42:  Lowest    Pri.58:  Lowest
Pri.11: Lowest      Pri.27:  Lowest    Pri.43:  Lowest    Pri.59:  Lowest
Pri.12: Lowest      Pri.28:  Lowest    Pri.44:  Lowest    Pri.60:  Lowest
Pri.13: Lowest      Pri.29:  Lowest    Pri.45:  Lowest    Pri.62:  Lowest
Pri.14: Lowest      Pri.30:  Lowest    Pri.46:  Lowest    Pri.62:  Lowest
Pri.15: Lowest      Pri.31:  Lowest    Pri.47:  Lowest    Pri.63:  Lowest

                                                                   [Apply]
                              TOS Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                   [Esc] Previous Menu
```

TOS Configuration interface

SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks on the Internet.

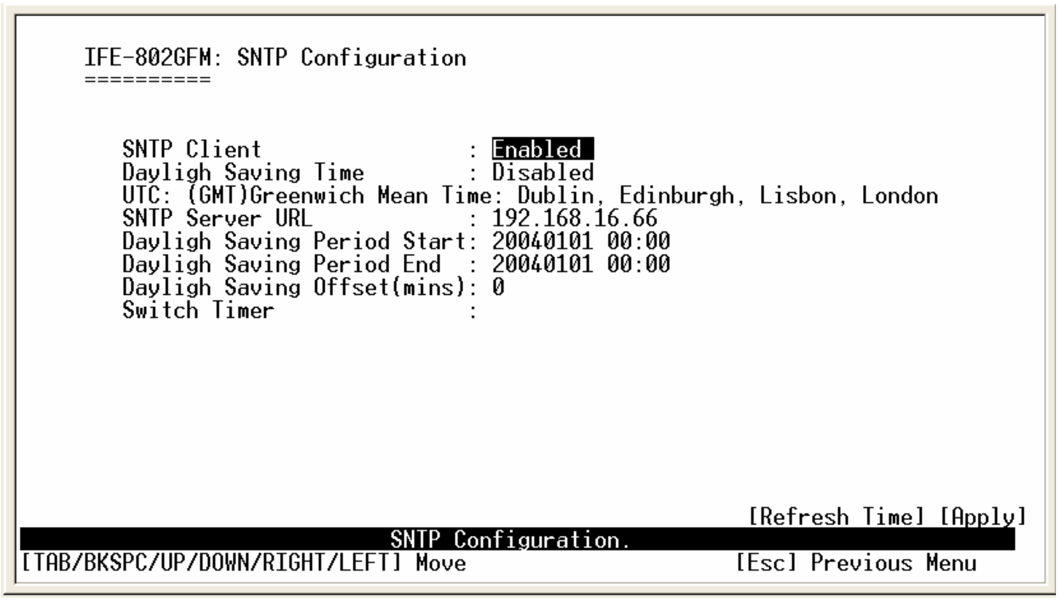
1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable the daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zones for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	-1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am

EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm

JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** display the switch current time.
8. And then, select the **<Apply>** to save the configuration
9. To refresh the time information, select **<Refresh Time>**



```
     IFE-802GFM: SNTP Configuration
     ==========

        SNTP Client                : Enabled
        Dayligh Saving Time        : Disabled
        UTC: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
        SNTP Server URL            : 192.168.16.66
        Dayligh Saving Period Start: 20040101 00:00
        Dayligh Saving Period End  : 20040101 00:00
        Dayligh Saving Offset(mins): 0
        Switch Timer               :

                                                       [Refresh Time] [Apply]
                              SNTP Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                   [Esc] Previous Menu
```

SNTP Configuration interface

IGMP Configuration

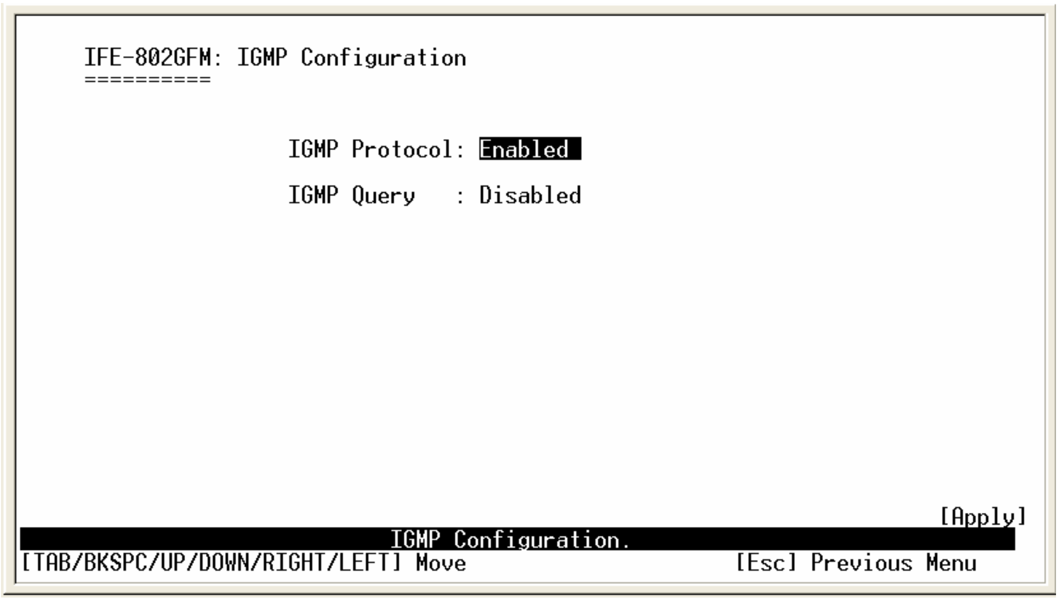
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of messages.

Message	Description
Query	A message sent from the querier (IGMP router or switch) that requests a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

IGMP Configuration

If the switch supports IP multicasts, you can enable IGMP protocol. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be displayed in the IGMP status section.

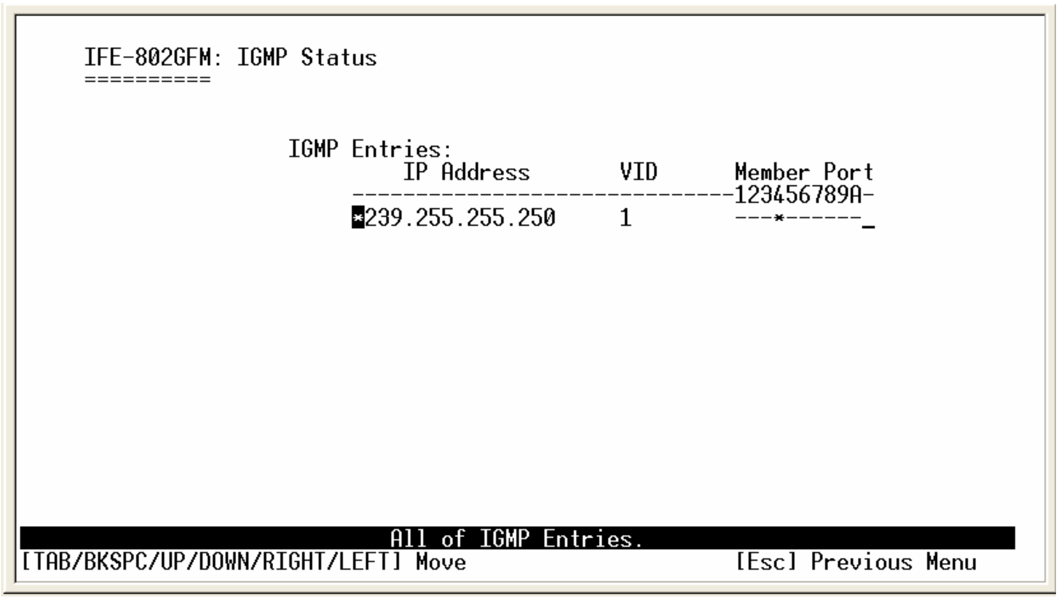


```
     IFE-802GFM: IGMP Configuration
     ==========

                     IGMP Protocol: Enabled

                     IGMP Query   : Disabled










                                                                      [Apply]
                              IGMP Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

IGMP Configuration interface

IGMP Status

When you enable the IGMP query you will see the information shown below.



```
     IFE-802GFM: IGMP Status
     ==========

                     IGMP Entries:
                          IP Address       VID      Member Port
                          ------------------------------123456789A-
                          *239.255.255.250     1        ---*------_









                              All of IGMP Entries.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

IGMP Status interface

X Ring Redundancy

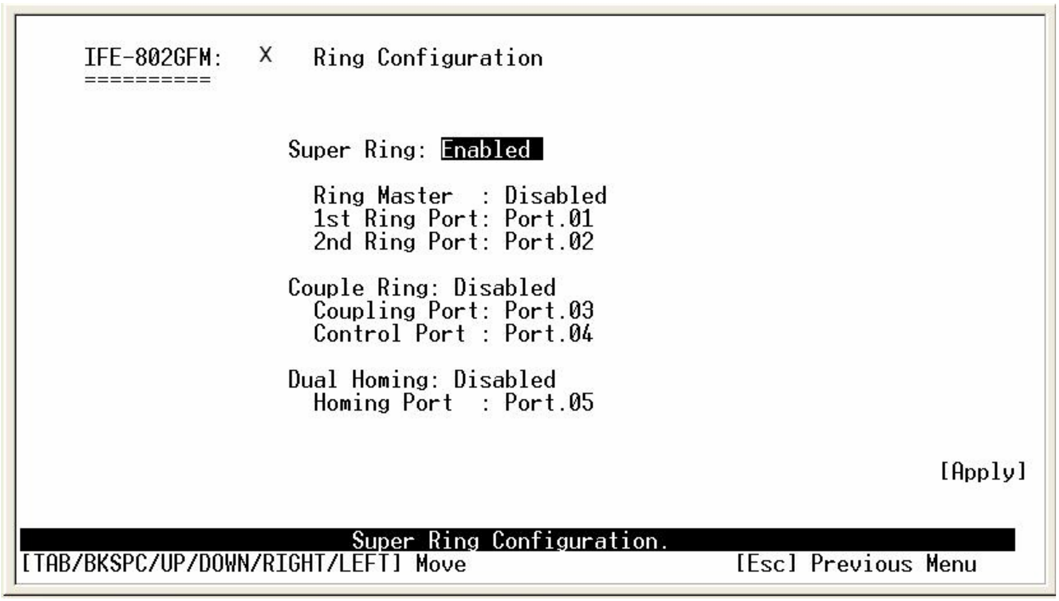
The X-ring provides a faster redundant recovery method than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithm is not the same and the cabling is simpler.

In the X-ring topology, every switch should have the X-ring function enabled and two member ports assigned on the switch. Each switch in the X-ring group uses two ports to enable the ring. The X-Ring topology 'daisy chains' the switches' member ports, to the next switch in the ring – one connection to the switch on the right, one connection to the switch on the left. Other switches are called working switches and their two member ports are called working ports. When a failure of a network connection occurs, the backup port will automatically become a working port to continue the communication.
The switch can be set as the ring master or slave. The ring master can negotiate and send commands to the other switches in the X-ring group. If there are 2 or more switches are in master mode (not recommended), then the software will select the switch with lowest MAC address number as the ring master. Select only one switch as the Ring Master.

The system also supports the ring coupling that can connect 2 or more X-ring groups for the redundant backup function and dual homing function that prevents connection loss between X-ring groups and upper level/core switches.

- **X-ring:** To enable the X-ring function
- **Ring Master:** Enable means the switch is ring master. Disable means the switch is slave
- **1st & 2nd Ring Ports:** Select two ports as the member ports. One of the ports will be the working port and the other port will be the backup port. The system will automatically decide the working port and the backup port.
- **Coupling Ring:** To enable the coupling ring function
- **Coupling port:** Select the member port
- **Control port:** Select the switch as the master switch in the coupling ring
- **Dual Homing:** To enable the Dual Homing function
- **Homing port:** Set up one of the ports on the switch to be the Dual Homing port. In an X-ring group, the maximum Dual Homing port is one. Dual Homing can only work when the X-ring function is enabled.

- Select the **<Apply>** to save the configuration



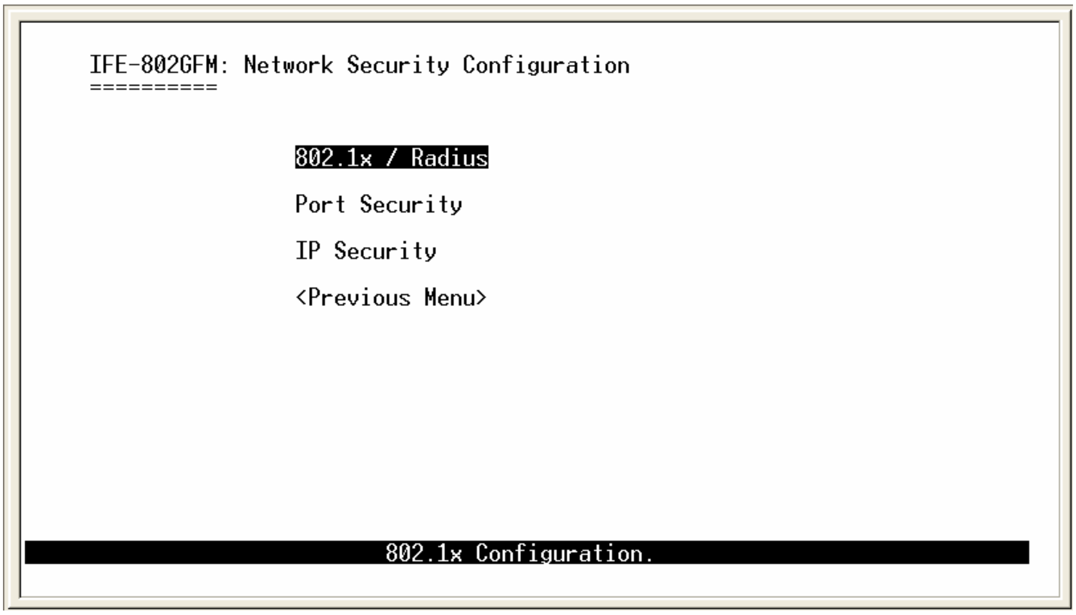
```
     IFE-802GFM:   X   Ring Configuration
     ==========

                    Super Ring: Enabled

                      Ring Master   : Disabled
                      1st Ring Port: Port.01
                      2nd Ring Port: Port.02

                    Couple Ring: Disabled
                      Coupling Port: Port.03
                      Control Port : Port.04

                    Dual Homing: Disabled
                      Homing Port   : Port.05

                                                                      [Apply]

                                  Super Ring Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                      [Esc] Previous Menu
```

Super ring Interface

[NOTE] When you enable the X-ring function, you must disable the RSTP. The X-ring function and RSTP function cannot exist at the same time.

Security Configuration

In this section, you can configure 802.1x, IP, and port security.

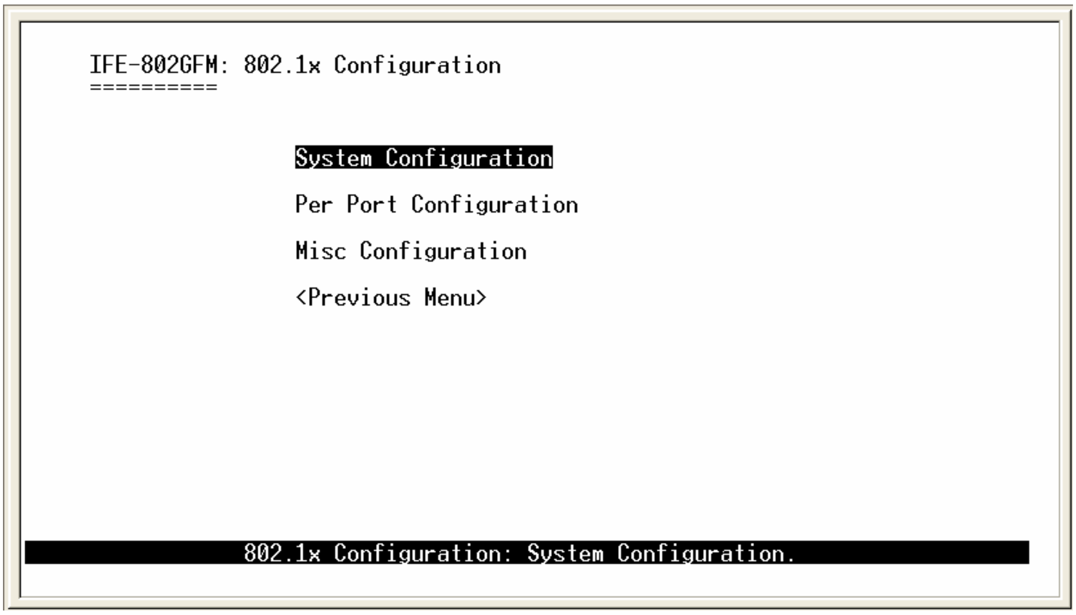


```
IFE-802GFM: Network Security Configuration
==========

                    802.1x / Radius
                    Port Security
                    IP Security
                    <Previous Menu>

                      802.1x Configuration.
```

Security Configuration interface

802.1X/ Radius Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.



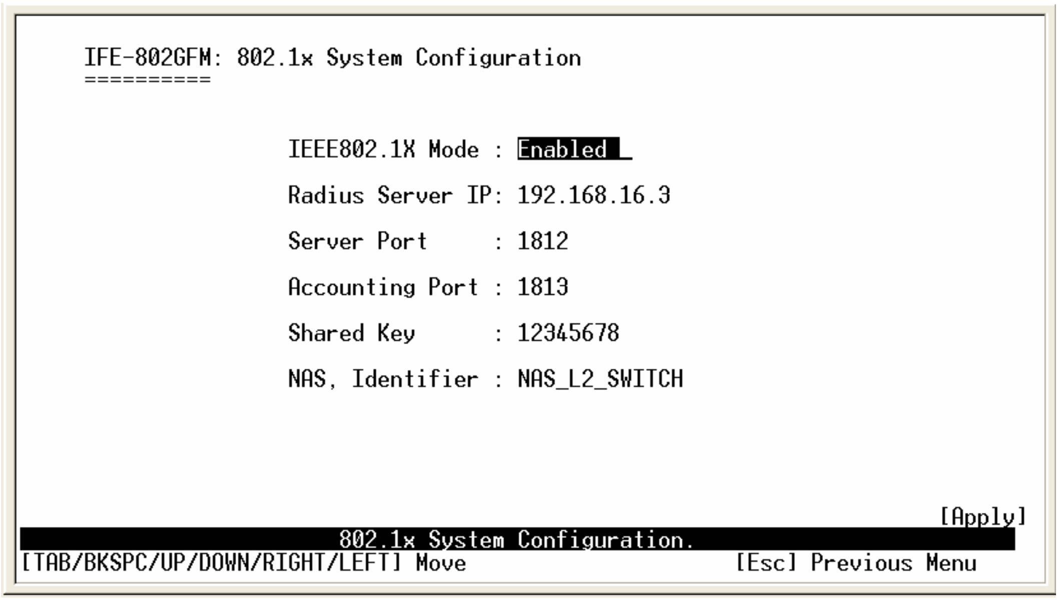
```
IFE-802GFM: 802.1x Configuration
==========

                System Configuration

                Per Port Configuration

                Misc Configuration

                <Previous Menu>






              802.1x Configuration: System Configuration.
```

802.1x Configuration interface

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x mode:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. **Apply** the configuration.



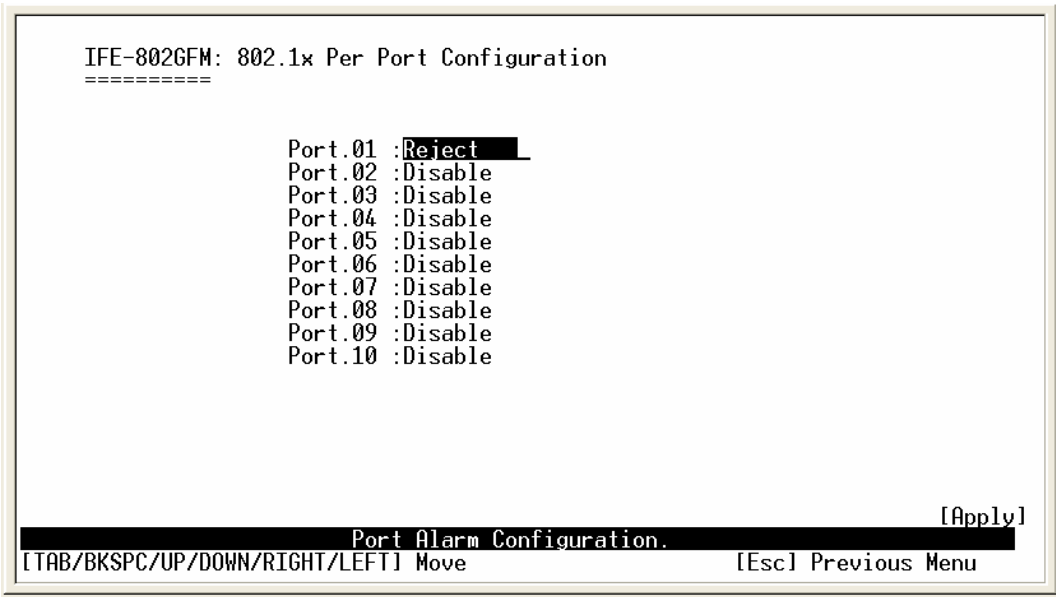
```
IFE-802GFM: 802.1x System Configuration
==========

                IEEE802.1X Mode : Enabled
                Radius Server IP: 192.168.16.3
                Server Port     : 1812
                Accounting Port : 1813
                Shared Key      : 12345678
                NAS, Identifier : NAS_L2_SWITCH

                                                                  [Apply]
                          802.1x System Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

802.1x System Configuration interface

802.1x Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use the "**Space**" key change the state value.

- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Select the **<Apply>** to save the configuration

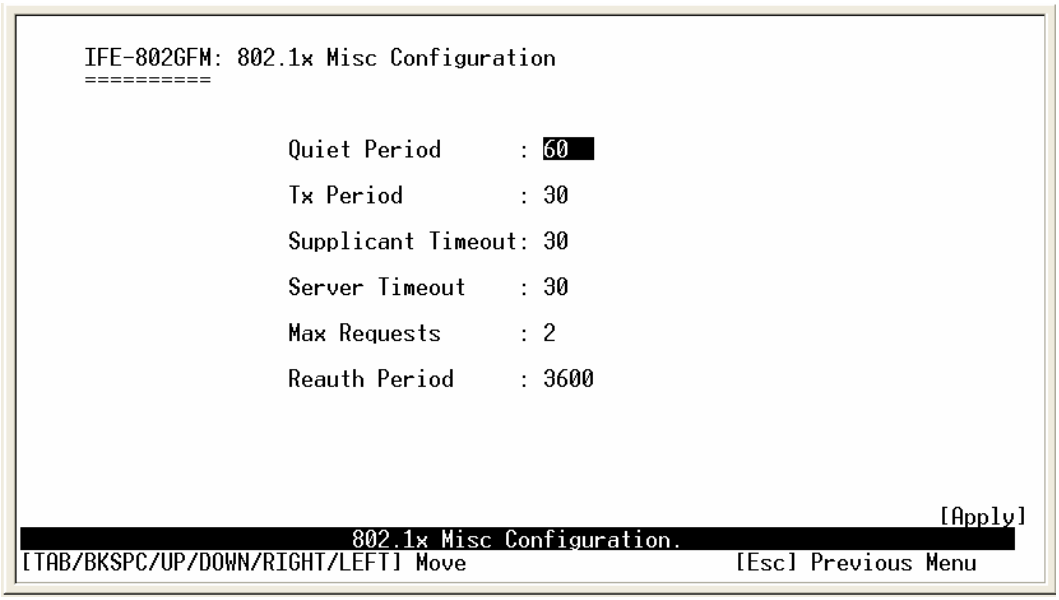


```
     IFE-802GFM: 802.1x Per Port Configuration
     ==========


                         Port.01 :Reject
                         Port.02 :Disable
                         Port.03 :Disable
                         Port.04 :Disable
                         Port.05 :Disable
                         Port.06 :Disable
                         Port.07 :Disable
                         Port.08 :Disable
                         Port.09 :Disable
                         Port.10 :Disable







                                                                  [Apply]
                                        Port Alarm Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                     [Esc] Previous Menu
```

802.1x Per Port Setting interface

Miscellaneous Configuration

1. **Quiet Period:** set the period during which the port does not try to acquire a supplicant.
2. **TX Period:** set the period the port waits for the next re-transmit of EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentications that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which connected clients must be re-authenticated.
7. Select **<Apply>**

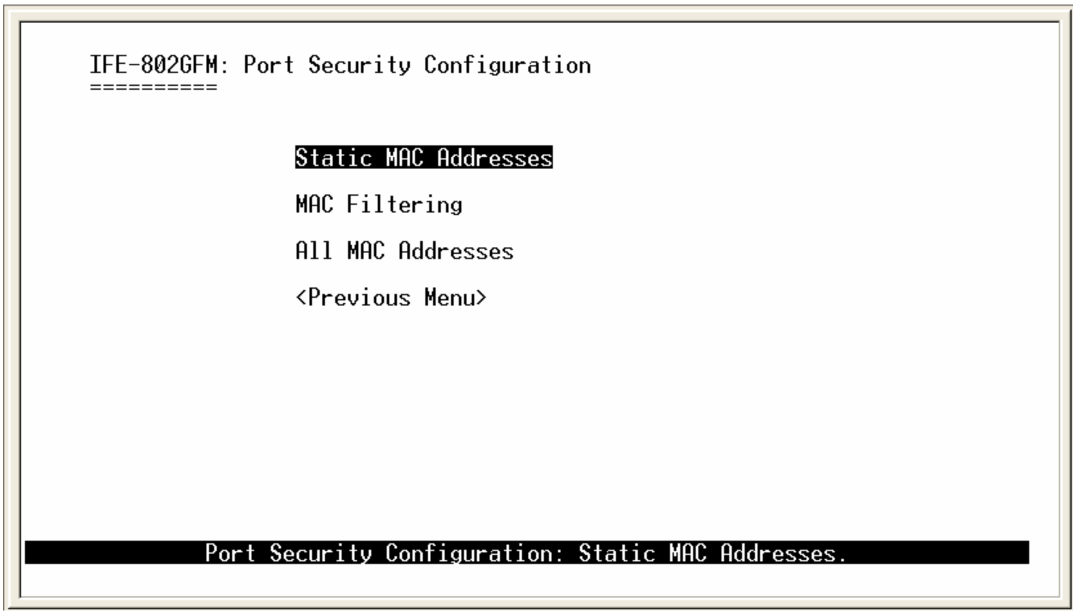


```
IFE-802GFM: 802.1x Misc Configuration
==========

                Quiet Period      : 60
                Tx Period         : 30
                Supplicant Timeout: 30
                Server Timeout    : 30
                Max Requests      : 2
                Reauth Period     : 3600

                                                                   [Apply]
                          802.1x Misc Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                  [Esc] Previous Menu
```

802.1x Misc Configuration interface

Port Security

Use the MAC address to ensure port security.



```
IFE-802GFM: Port Security Configuration
==========

                Static MAC Addresses
                MAC Filtering
                All MAC Addresses
                <Previous Menu>



              Port Security Configuration: Static MAC Addresses.
```

MAC Address Configuration interface

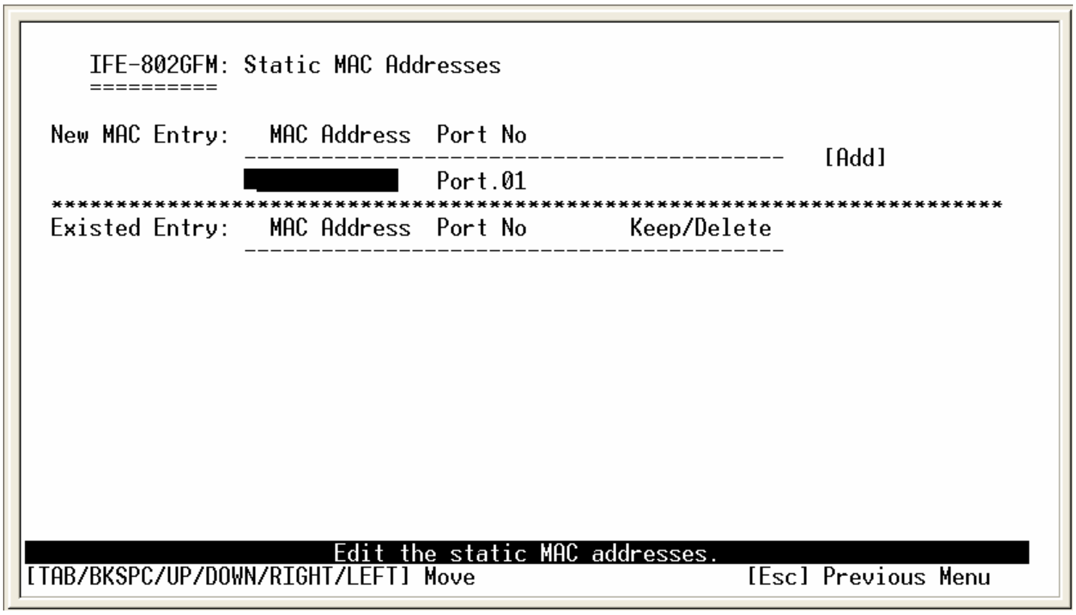
Static MAC Address

You can add a static MAC address: it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

- **Add the Static MAC Address**

You can add a static MAC address in the switch MAC table.

1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
2. **Port No.:** press “**Space**” key to select the port number.
3. Select **<Add>** to save all configured values.
4. **Existed Entry:** you will see the added MAC address information in the Exited Entry table. You can delete or keep the added MAC address.
5. Select **<Apply>** to apply the configuration.

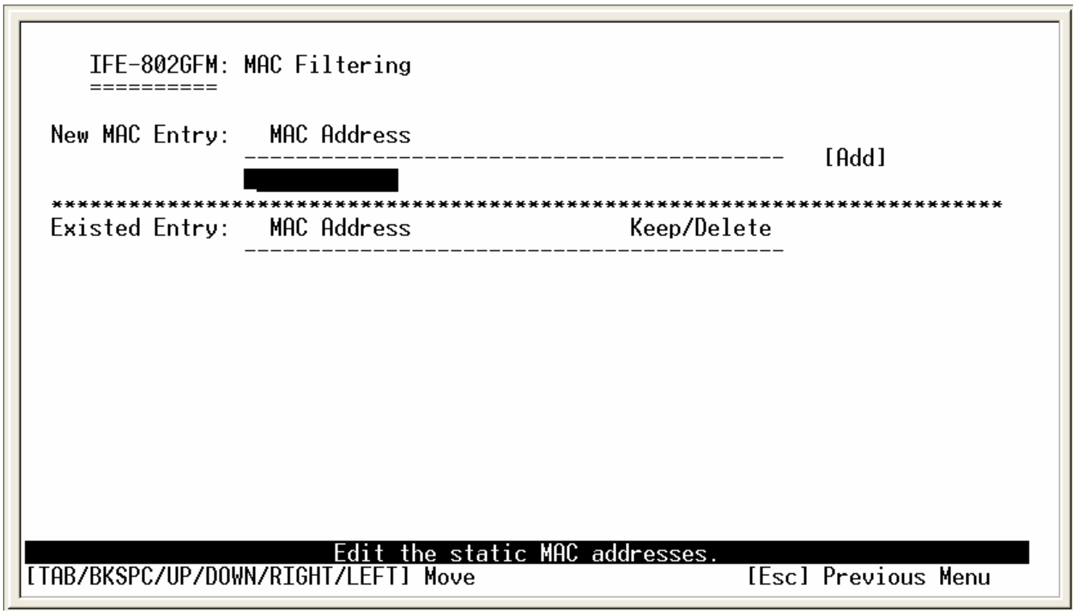


```
    IFE-802GFM: Static MAC Addresses
    ==========

  New MAC Entry:   MAC Address  Port No
                 ------------------------------------------   [Add]
                                Port.01
*************************************************************************
  Existed Entry:   MAC Address  Port No       Keep/Delete
                 ------------------------------------------









                        Edit the static MAC addresses.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

Static MAC Address interface

Filtering MAC Addresses

By filtering MAC addresses, the switch can easily filter pre-configured MAC addresses and enhance security. You can add and delete MAC addresses to be filtered.



```
   IFE-802GFM: MAC Filtering
   ==========

 New MAC Entry:   MAC Address
                 ------------------------------------------   [Add]

************************************************************************
 Existed Entry:   MAC Address                 Keep/Delete
                 ------------------------------------------

                        Edit the static MAC addresses.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

Filtering MAC Address interface

- **Add the Filtering MAC Addresses**

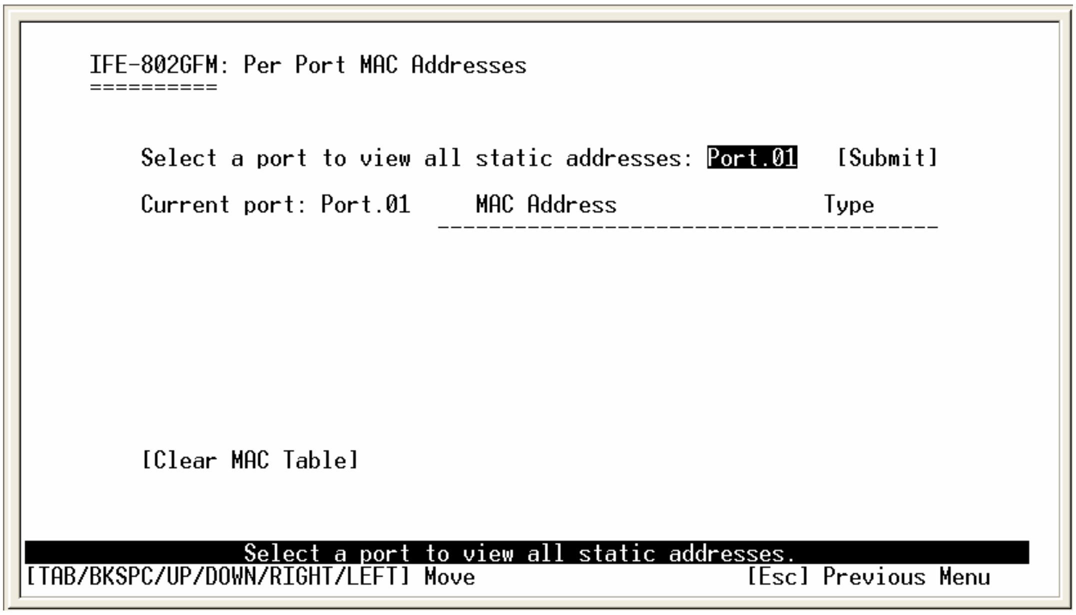
1. **MAC Address:** Enter the MAC address that you want to filter.
2. Select **<Add>** to save all configured values.

- **Existed Entry:** you will see the added MAC address information in the Exited Entry table. You can delete or keep the added MAC addresses
- Select **<Apply>** to apply the configuration.

All MAC Addresses

You can view the port that is connected to the device's MAC address and related devices' MAC addresses.

1. Select the port and **[Submit]**.



```
    IFE-802GFM: Per Port MAC Addresses
    ==========

        Select a port to view all static addresses: Port.01   [Submit]

        Current port: Port.01     MAC Address                Type
                                 ---------------------------------------



        [Clear MAC Table]

                    Select a port to view all static addresses.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                     [Esc] Previous Menu
```

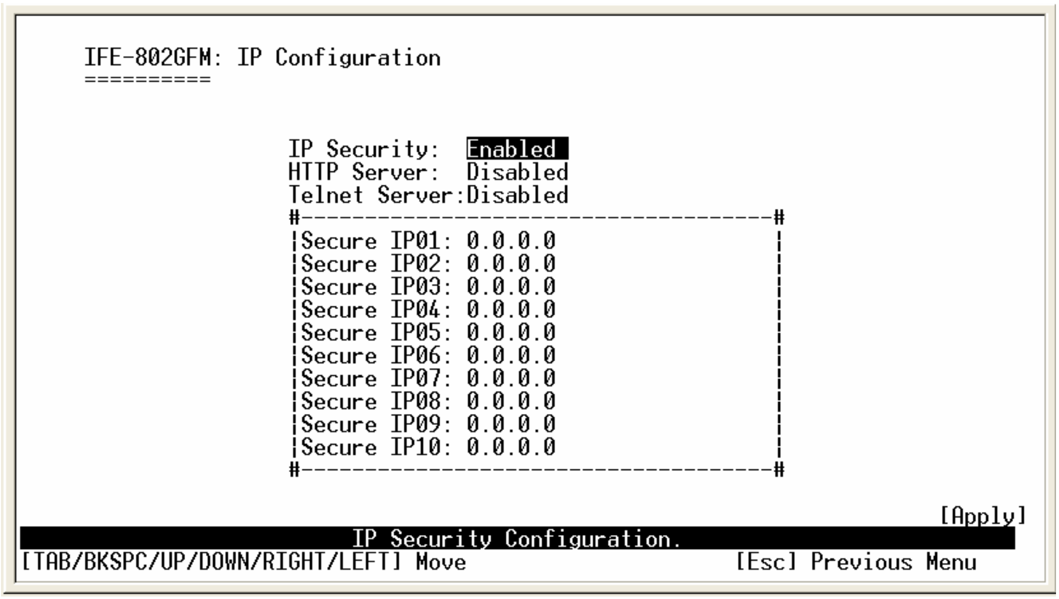
All MAC Address interface

2. The selected port of the static MAC address information is displayed.
3. Select the **[Clear MAC Table]** to clear the current port static MAC address information on the screen.

IP Security

The IP security function allows the user to assign 10 specific IP addresses which have permission to access the switch through the web browser and remote telnet interface for managing the switch.

- **IP Security:** To enable the IP security function
- HTTP Server: To enable the HTTP function for allowing user access the system through the web browser
- Telnet Server: To enable the Telnet function for allowing user access the system by the remote telnet interface
- **Security IP 1 ~ 10:** Assign up to 10 specific IP addresses. Only these 10 IP addresses can access and manage the switch through the Web browser and telnet interface



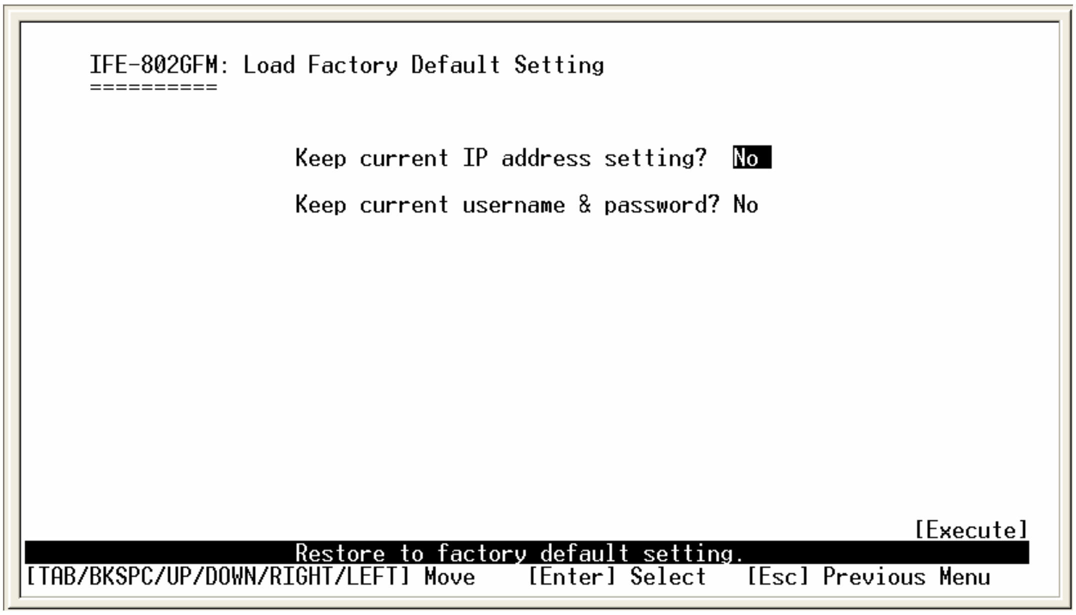
```
    IFE-802GFM: IP Configuration
    ==========


                        IP Security:  Enabled
                        HTTP Server:  Disabled
                        Telnet Server:Disabled
                        #--------------------------------------#
                        |Secure IP01: 0.0.0.0                  |
                        |Secure IP02: 0.0.0.0                  |
                        |Secure IP03: 0.0.0.0                  |
                        |Secure IP04: 0.0.0.0                  |
                        |Secure IP05: 0.0.0.0                  |
                        |Secure IP06: 0.0.0.0                  |
                        |Secure IP07: 0.0.0.0                  |
                        |Secure IP08: 0.0.0.0                  |
                        |Secure IP09: 0.0.0.0                  |
                        |Secure IP10: 0.0.0.0                  |
                        #--------------------------------------#

                                                              [Apply]
                              IP Security Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                 [Esc] Previous Menu
```

IP Security interface

Loading Factory Default Settings

To reset switch to the default configuration.

- **Keep current IP address setting?:** you can decide to keep the current IP address or reset to the default IP address. Use the **Space** key to mark the selection.
- **Keep current username and password?:** you can decide to keep the current username and password or reset to the default username and password. Use the **Space** key to mark the selection.
- After the selection, **[Execute]** to reset.

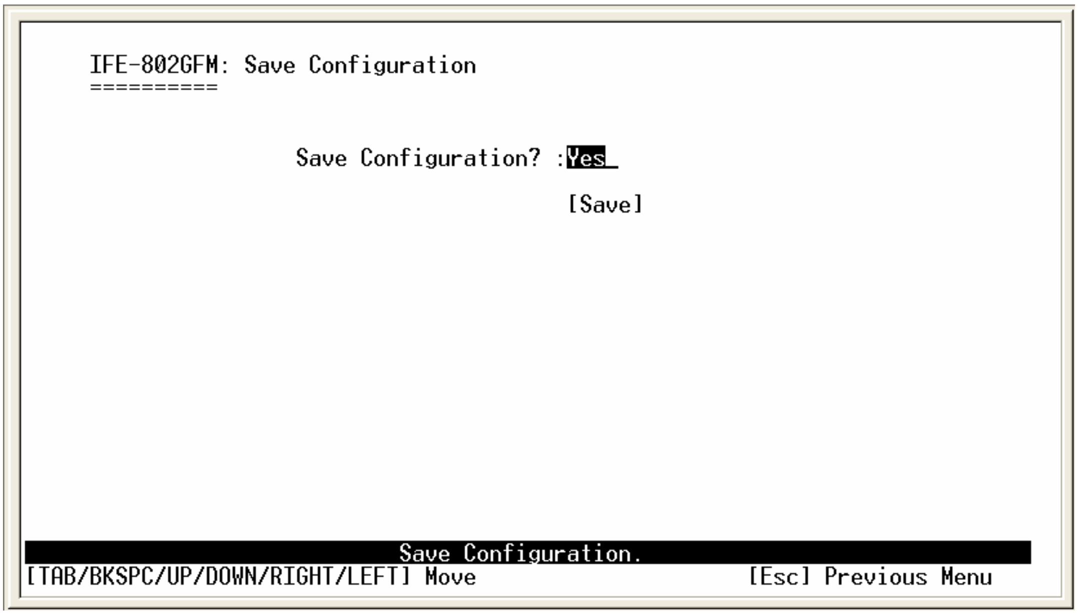


```
IFE-802GFM: Load Factory Default Setting
==========

                Keep current IP address setting?  No
                Keep current username & password? No










                                                              [Execute]
                      Restore to factory default setting.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move    [Enter] Select   [Esc] Previous Menu
```

Load Factory Default Setting interface

Saving the Configuration

To save the changes and settings that you have made in the system and to ensure the configuration will be saved, use the **Space** key to select the options – **Yes** or **No**. **Yes** means save all the configurations. **No** means do not save the configuration. After selecting the option, execute the **Save** action to save the configuration.

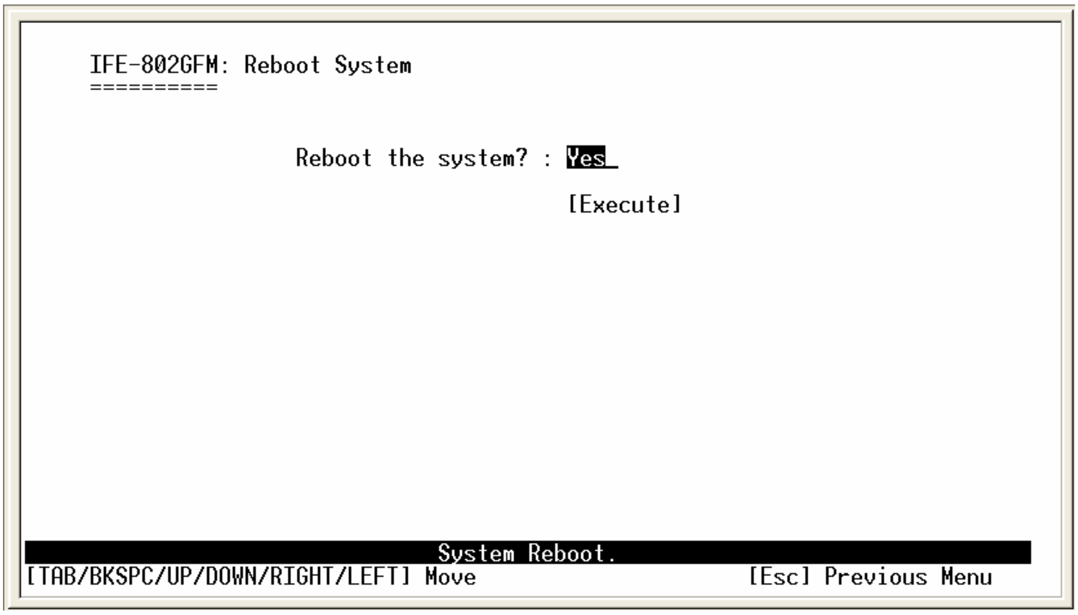


```
IFE-802GFM: Save Configuration
==========

                Save Configuration? :Yes_
                                     [Save]











                           Save Configuration.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

Save All Configuration interface

Rebooting the System

To reboot the switch in software, use the **Space** key to select the options – **Yes** or **No**. **Yes** means to reboot the system. **No** means do not reboot the system. Use the **Tab** key to move to **[Execute]** action and press the **Enter** key to reboot the system.



```
     IFE-802GFM: Reboot System
     ==========

                         Reboot the system? : Yes_
                                              [Execute]

                                System Reboot.
[TAB/BKSPC/UP/DOWN/RIGHT/LEFT] Move                    [Esc] Previous Menu
```

Reboot System interface

Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

On the CPU board of the switch there is an embedded HTML web site residing in flash memory, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 5.0. And, it is applied for Java Applets for reducing network bandwidth consumption, enhancing access speed and presenting an easy viewing screen.

[NOTE] By default, IE5.0 or later version does not allow Java Applets to activate sockets. The user has to explicitly modify the browser setting to enable Java Applets to operate network ports*. **Use IE6.0 or later for ease of use.***

Preparing for Web Management

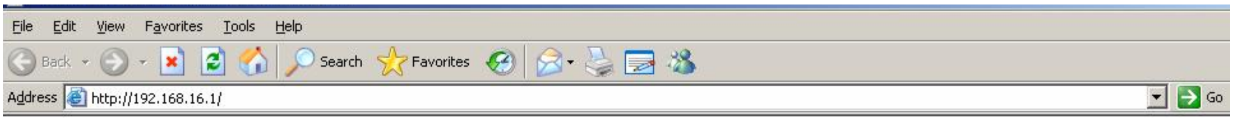
Before using the web management, install the industrial switch on the network and make sure that any PC on the network can connect with the industrial switch through the web browser. The industrial switch default IP address, subnet mask, username and password are:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**

- User Name: **root**
- Password: **root**

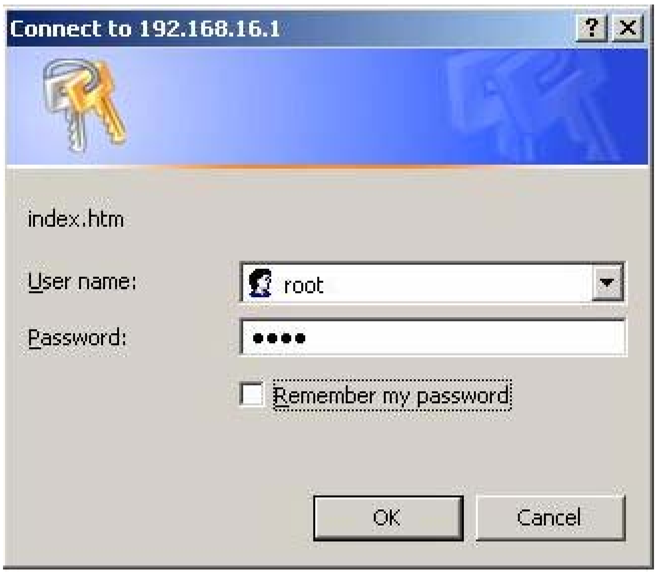
System Login

1. Launch the Internet Explorer on the PC
2. Key in "http:// "+" the IP address of the switch", and then Press "**Enter**".



Address http://192.168.16.1/

3. The login screen will appear
4. Key in the user name and password. The default user name and password are the same **-** "**root**"
5. Press "**Enter**" or "**OK**", and then the home screen of the Web-based management appears as below:



Connect to 192.168.16.1

index.htm

User name: root

Password: ●●●●

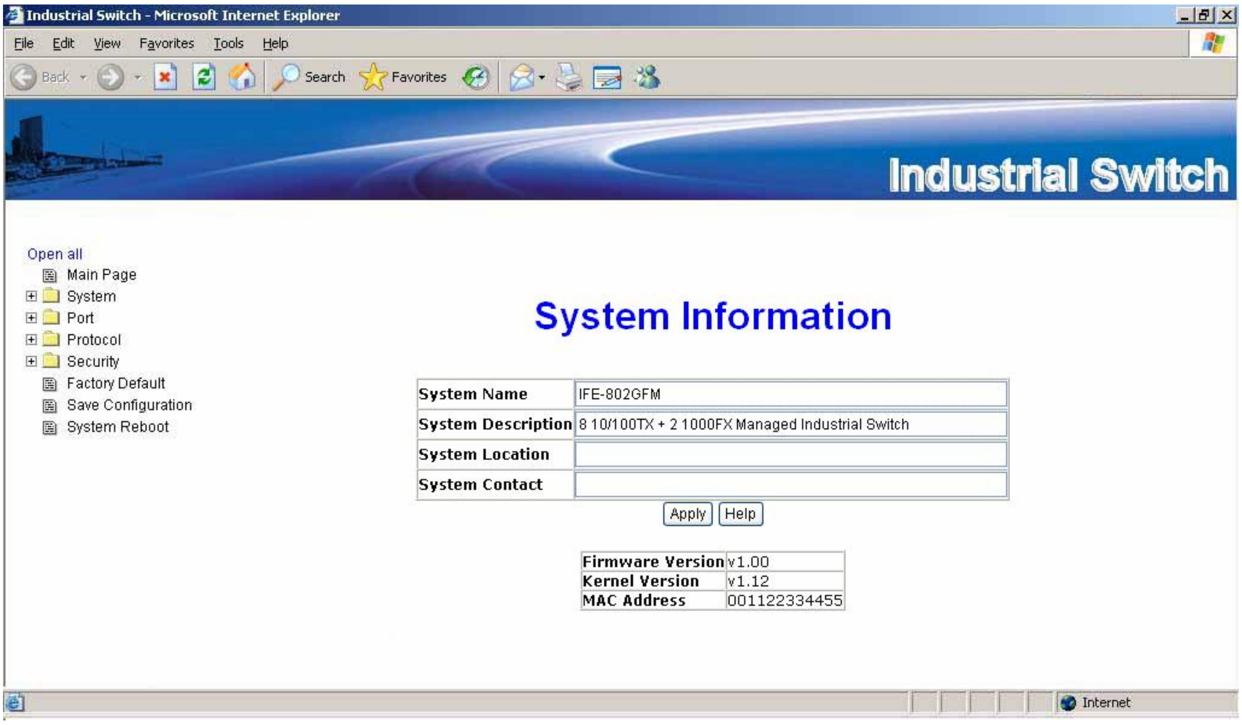
☐ Remember my password

Login screen

System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 64 bytes
- **System Description:** Displays the description of switch. **Read only** cannot be modified
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes
- **System Contact:** Enter the name of contact person or organization
- **Firmware Version:** Display the switch’s firmware version
- **Kernel Version:** Display the kernel software version
- **MAC Address:** Display the unique hardware address assigned by manufacturer (default)



System Information

System Name	IFE-802GFM
System Description	8 10/100TX + 2 1000FX Managed Industrial Switch
System Location	
System Contact	

Firmware Version	v1.00
Kernel Version	v1.12
MAC Address	001122334455

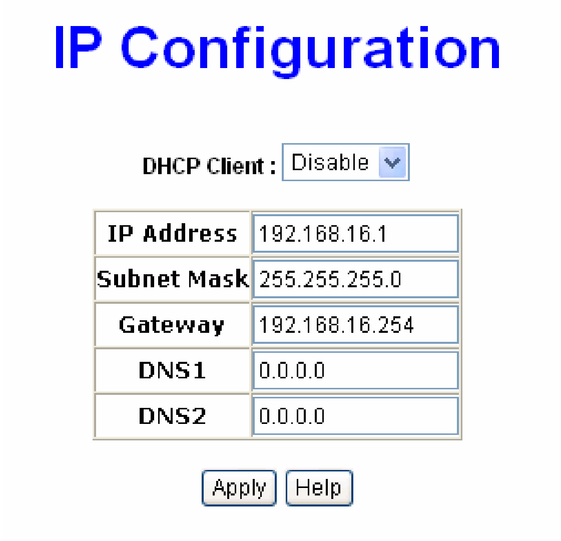
Switch settings interface

IP Configuration

The user can configure the IP Settings and DHCP client function

- **DHCP Client:** To enable or disable the DHCP client function. When DHCP client function is enabled, the industrial switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the DHCP server assigned IP address. After clicking the “Apply” button, a popup dialog appears. It is to inform the user that when the DHCP client is enabled, the current IP will be lost and the user should find the new IP on the DHCP server. To cancel enabling the DHCP client function, click “cancel”

- **IP Address:** To assign an IP address by the user. If the DHCP client function is enabled, then the user does not need to assign an IP address because the DHCP server will assign the IP address for the industrial switch and display it in this column. The default IP address is 192.168.16.1
- **Subnet Mask:** Assign the subnet mask of the IP address. If the DHCP client function is enabled, then the user does not need to assign the subnet mask
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.16.254
- **DNS1:** Assign the primary DNS IP address
- **DNS2:** Assign the secondary DNS IP address
- And then, click Apply



IP Configuration

DHCP Client : Disable

IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS1	0.0.0.0
DNS2	0.0.0.0

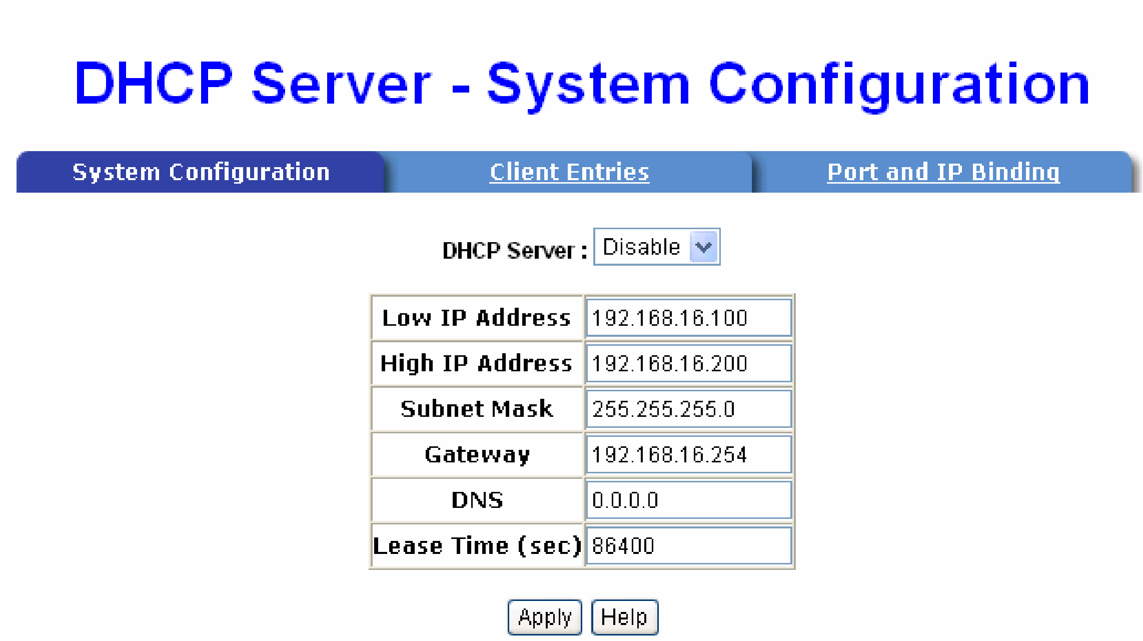
IP configuration interface

DHCP Server – System configuration

The system provides the DHCP server function. Enabling the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enabled – the switch will be the DHCP server on your local network.

- **Low IP Address:** the dynamic IP assignment range. A low IP address is the beginning of the dynamic IP assignment range. For example: the dynamic IP assignment range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address.
- **High IP Address:** the dynamic IP assignment range. A high IP address is the end of the dynamic IP assignment range. For example: a dynamic IP assignment range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High IP address.
- **Subnet Mask:** the dynamic IP assignment range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that the system will reset the dynamic IP assignment to ensure the dynamic IP will not be occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server - System Configuration

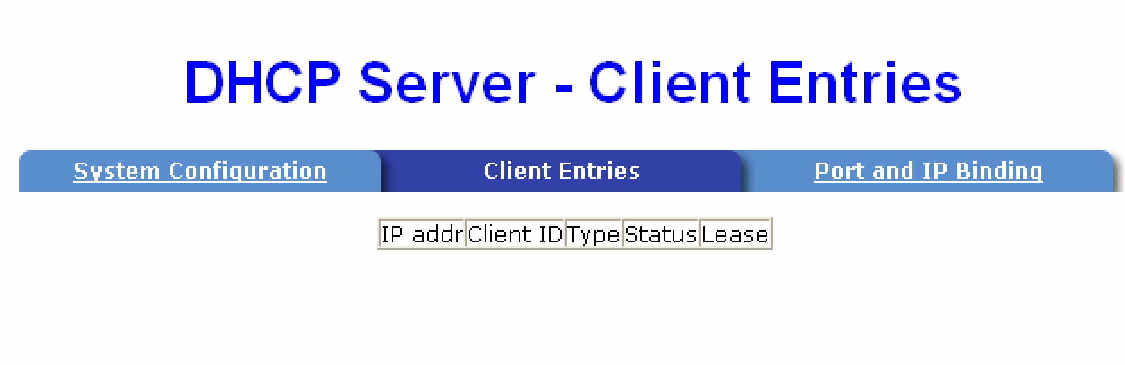
DHCP Server : Disable

Low IP Address	192.168.16.100
High IP Address	192.168.16.200
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS	0.0.0.0
Lease Time (sec)	86400

DHCP Server Configuration interface

DHCP Client – System Configuration

When the DHCP server function is active, the system will collect the DHCP client information and display it here.

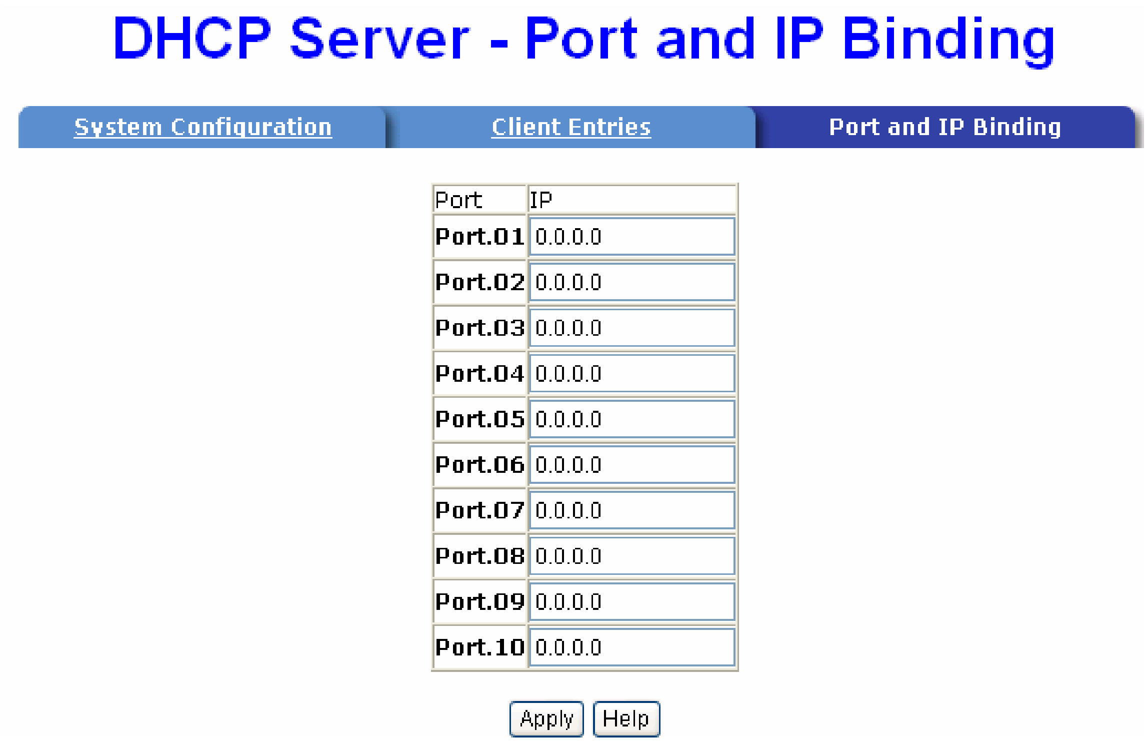


IP addr	Client ID	Type	Status	Lease

DHCP Client Entries interface

DHCP Server - Port and IP Bindings

You can assign the specific IP address that is the IP in dynamic IP assignment range to the specific port. When the device is connecting to the port and asks for dynamic IP assignment, the system will assign the IP address that has been assigned before to the connected device.



Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0

Port and IP Bindings interface

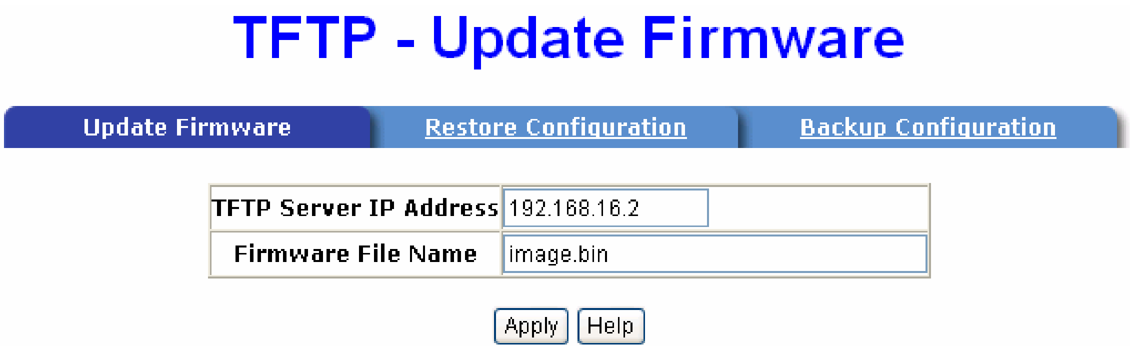
TFTP - Update Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** fill in your TFTP server IP.

2. **Firmware File Name:** the name of firmware image.

3. Click Apply.


TFTP - Update Firmware

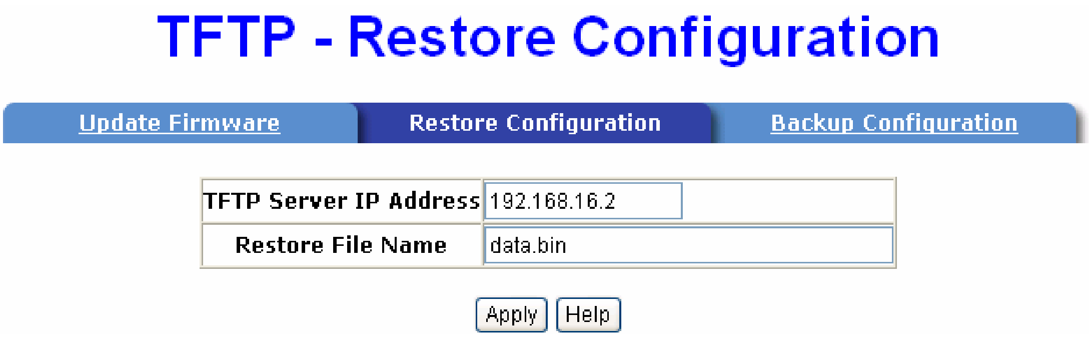
TFTP Server IP Address	192.168.16.2
Firmware File Name	image.bin

Update Firmware interface

TFTP – Restore Configuration

You can restore the EEPROM value from the TFTP server, but you must restore the image in TFTP server, switch will download the flash image.

1. **TFTP Server IP Address:** fill in the TFTP server IP address.
2. **Restore File Name:** fill in the correct restore file name.
3. Click Apply.


TFTP - Restore Configuration

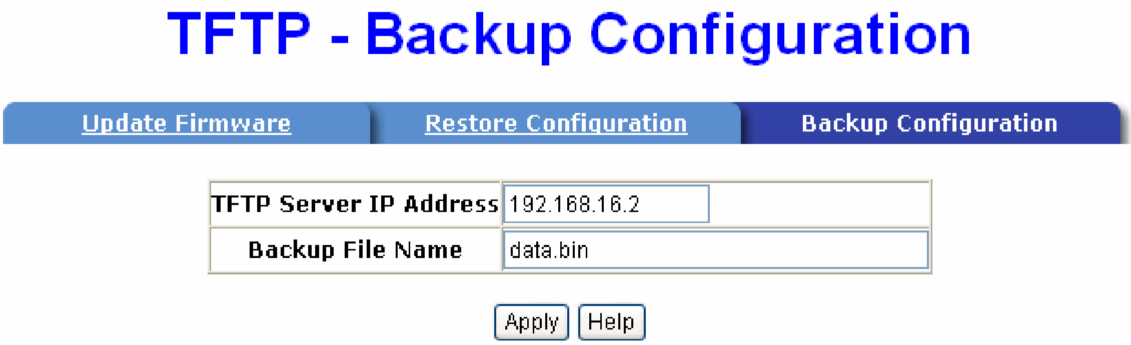
TFTP Server IP Address	192.168.16.2
Restore File Name	data.bin

Restore Configuration interface

TFTP – Backing up a Configuration

You can save the current EEPROM value from the switch to the TFTP server, then go to the TFTP restore configuration page to restore the EEPROM value.

1. **TFTP Server IP Address:** fill in the TFTP server IP address
2. **Backup File Name:** fill in the file name
3. Click Apply.



TFTP - Backup Configuration

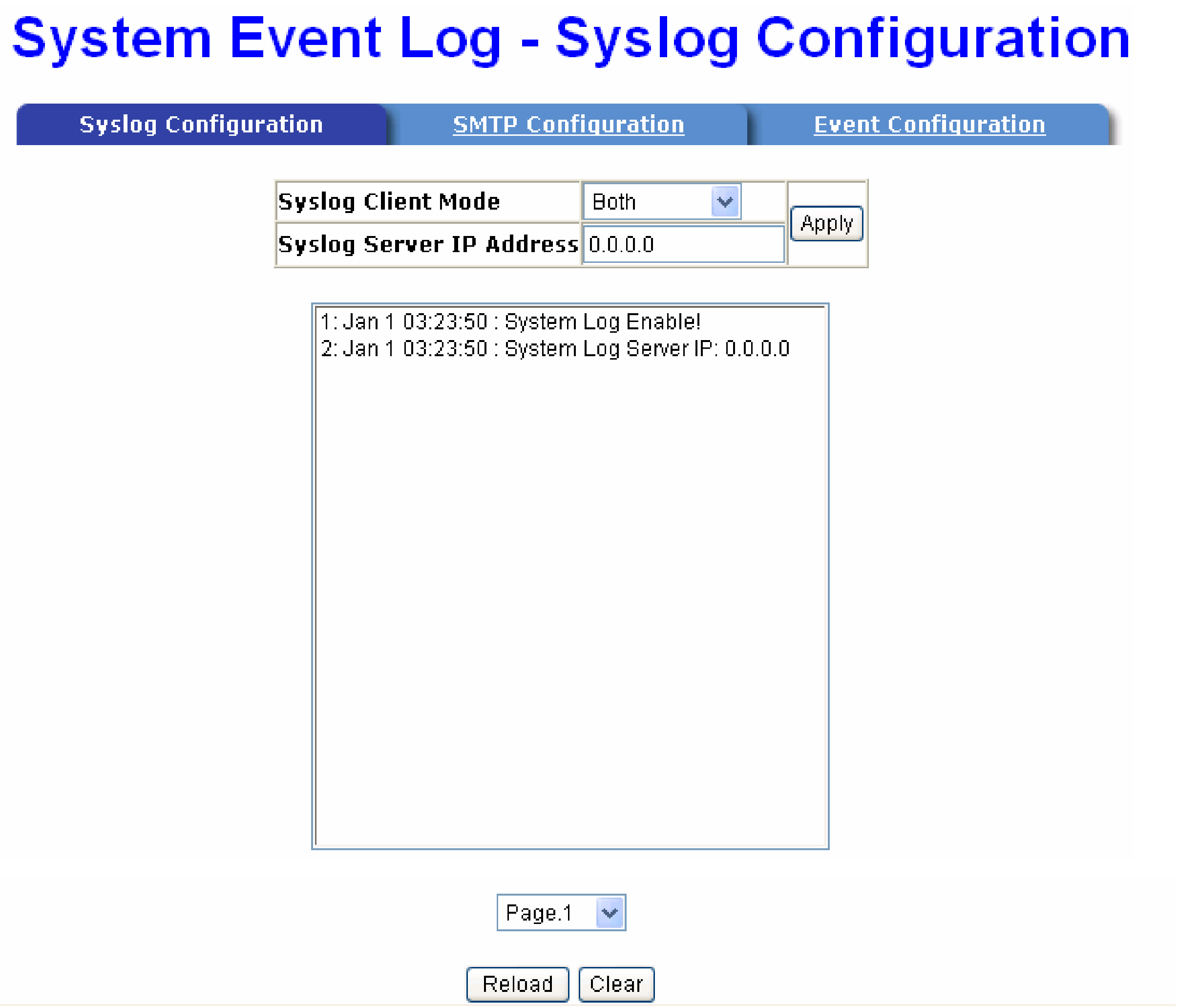
TFTP Server IP Address	192.168.16.2
Backup File Name	data.bin

Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode to be collected and stored in the system log server IP.

1. **Syslog Client Mode:** select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** assign the system log server IP address.
3. Click Reload to refresh the events log.
4. Click Clear to clear all current events log.
5. After configuring, Click Apply.



System Event Log - Syslog Configuration

Syslog Client Mode	Both	Apply
Syslog Server IP Address	0.0.0.0	

```
1: Jan 1 03:23:50 : System Log Enable!
2: Jan 1 03:23:50 : System Log Server IP: 0.0.0.0
```

Syslog Configuration interface

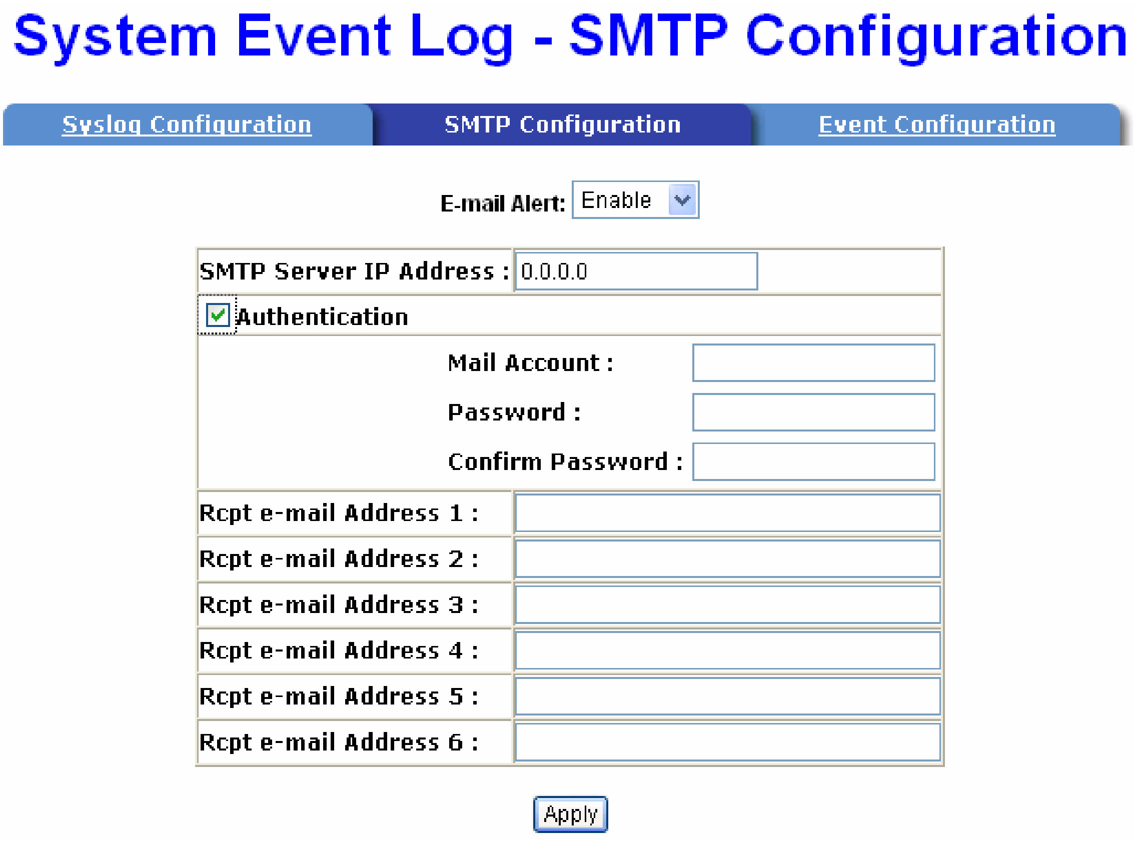
System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when the **Email Alert** is enabled, this function will then be available).
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when **Email Alert** enabled, this function will then be available).
4. **Mail Account:** set up the email account to receive the alert. Ex: mark.hendel@bmoc.com. It must be an existing email account on the mail server,

which you had set up in **SMTP Server IP Address** column.

5. **Password:** The email account password.
6. **Confirm Password:** reconfirm the password.
7. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
8. Click Apply.



System Event Log - SMTP Configuration

E-mail Alert: Enable

SMTP Server IP Address :	0.0.0.0
☑ Authentication	
Mail Account :	
Password :	
Confirm Password :	
Rcpt e-mail Address 1 :	
Rcpt e-mail Address 2 :	
Rcpt e-mail Address 3 :	
Rcpt e-mail Address 4 :	
Rcpt e-mail Address 5 :	
Rcpt e-mail Address 6 :	

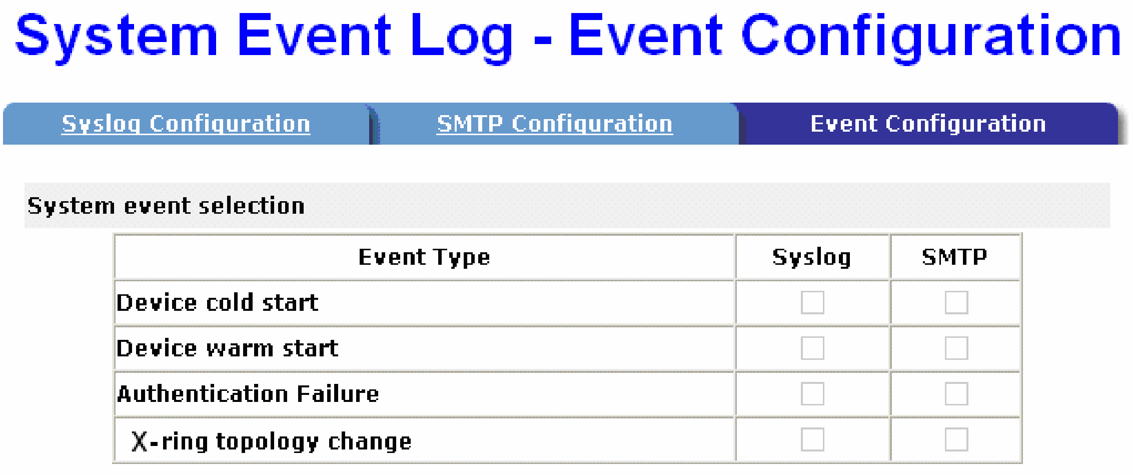
SMTP Configuration interface

System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, a port log and SMTP events can be selected. After configure, Click Apply.

- **System event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.

- **Device cold start:** when the device executes a cold start action, the system will issue a log event.
- **Device warm start:** when the device executes a warm start, the system will issue a log event.
- **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
- **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.

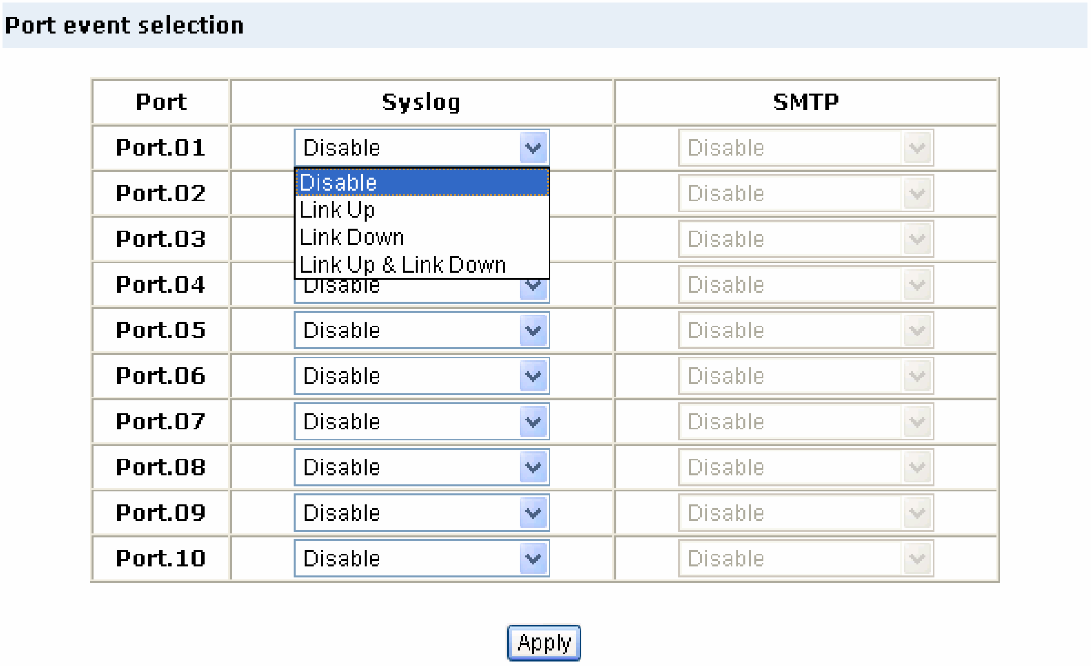


System Event Log - Event Configuration

System event selection

Event Type	Syslog	SMTP
Device cold start	□	□
Device warm start	□	□
Authentication Failure	□	□
X-ring topology change	□	□

- **Port event selection:** select the port events and port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.
  - **Link UP:** the system will issue a log message when port connection is up only.
  - **Link Down:** the system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.



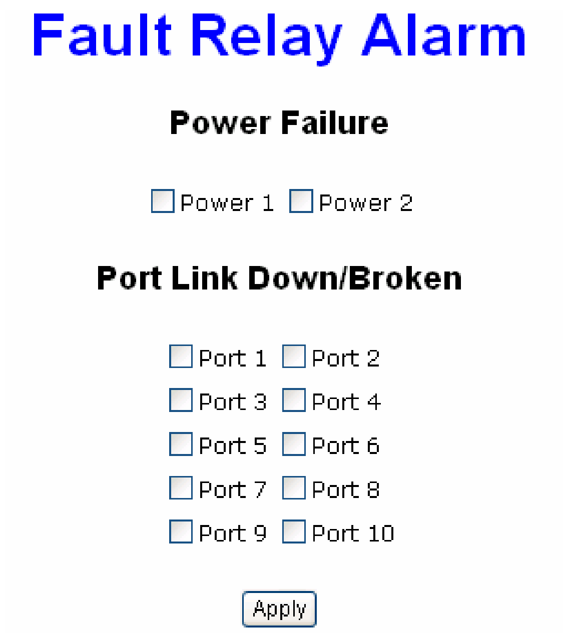
Port event selection

Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
Port.09	Disable	Disable
Port.10	Disable	Disable

Event Configuration interface

Fault Relay Alarm

- **Power Failure:** Mark the check box to enable the function of enabling the **FAULT** LED on the panel when power fails. The alarm contact will close.
- **Port Link Down/Broken:** Mark the check box to enable the function of enabling the **FAULT** LED on the panel when ports' link states are down. The alarm contact will close.



Fault Relay Alarm

Power Failure

□ Power 1 □ Power 2

Port Link Down/Broken

□ Port 1 □ Port 2
□ Port 3 □ Port 4
□ Port 5 □ Port 6
□ Port 7 □ Port 8
□ Port 9 □ Port 10

SNTP Configuration

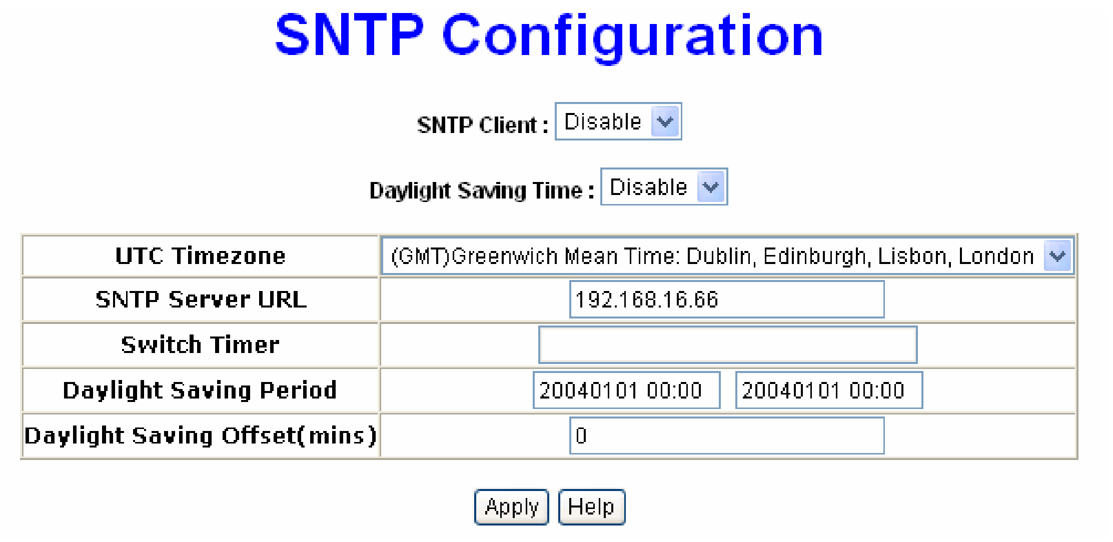
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks on the Internet.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian	-10 hours	2 am

Standard		
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** display the switch current time.
8. Click Apply.



SNTP Configuration

SNTP Client : Disable

Daylight Saving Time : Disable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server URL	192.168.16.66
Switch Timer	
Daylight Saving Period	20040101 00:00 20040101 00:00
Daylight Saving Offset(mins)	0

SNTP Configuration interface

IP Security

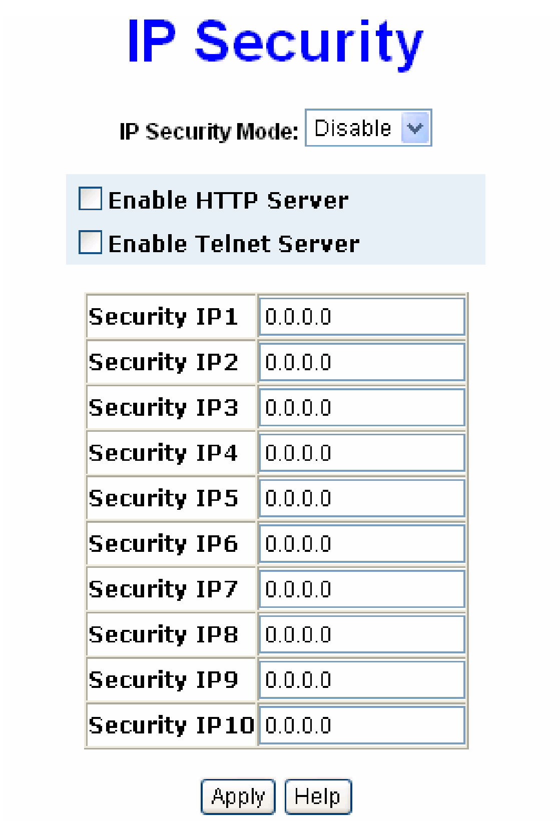
The IP security function allows the user to assign 10 specific IP addresses that have permission to access the switch through the web browser for secure switch management.

- **IP Security Mode:** when this option is in the **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access the switch via the HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access the switch via the telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP

addresses can access and manage the switch through the Web browser.

- And then, click Apply button to apply the configuration

[NOTE] Remember to execute the "Save Configuration" , otherwise the new configuration will be lost when the switch power is off.



IP Security

IP Security Mode: Disable

□ Enable HTTP Server

□ Enable Telnet Server

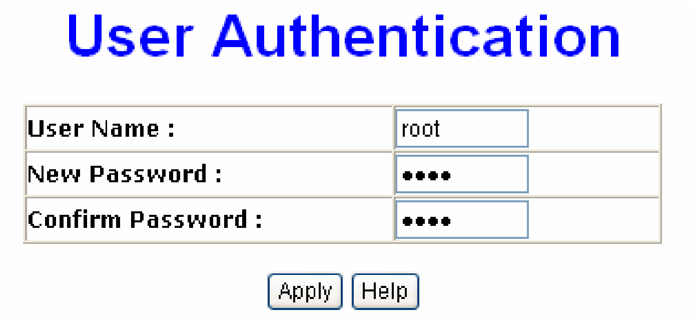
Security IP1	0.0.0.0
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

IP Security interface

User Authentication

To change web management login user name and password for the management security.

1. **User name:** Key in the new user name(The default is "root")
2. **Password:** Key in the new password(The default is "root")
3. **Confirm password:** Re-type the new password
4. And then, click Apply



User Authentication

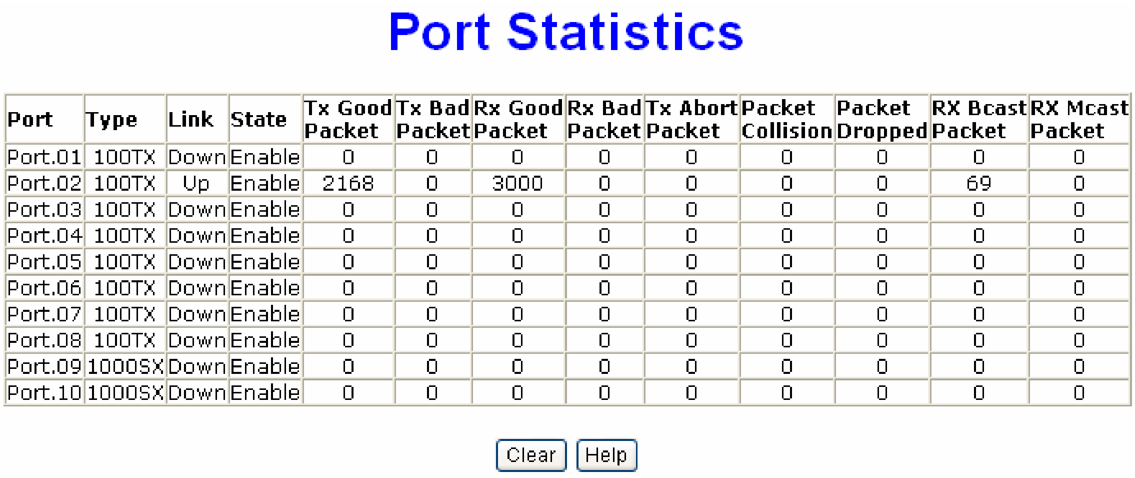
User Name :	root
New Password :	••••
Confirm Password :	••••

User Authentication interface

Port Statistics

The following information provides the current port statistic information

- Click Clear button to clean all counts



Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Up	Enable	2168	0	3000	0	0	0	0	69	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	1000SX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	1000SX	Down	Enable	0	0	0	0	0	0	0	0	0

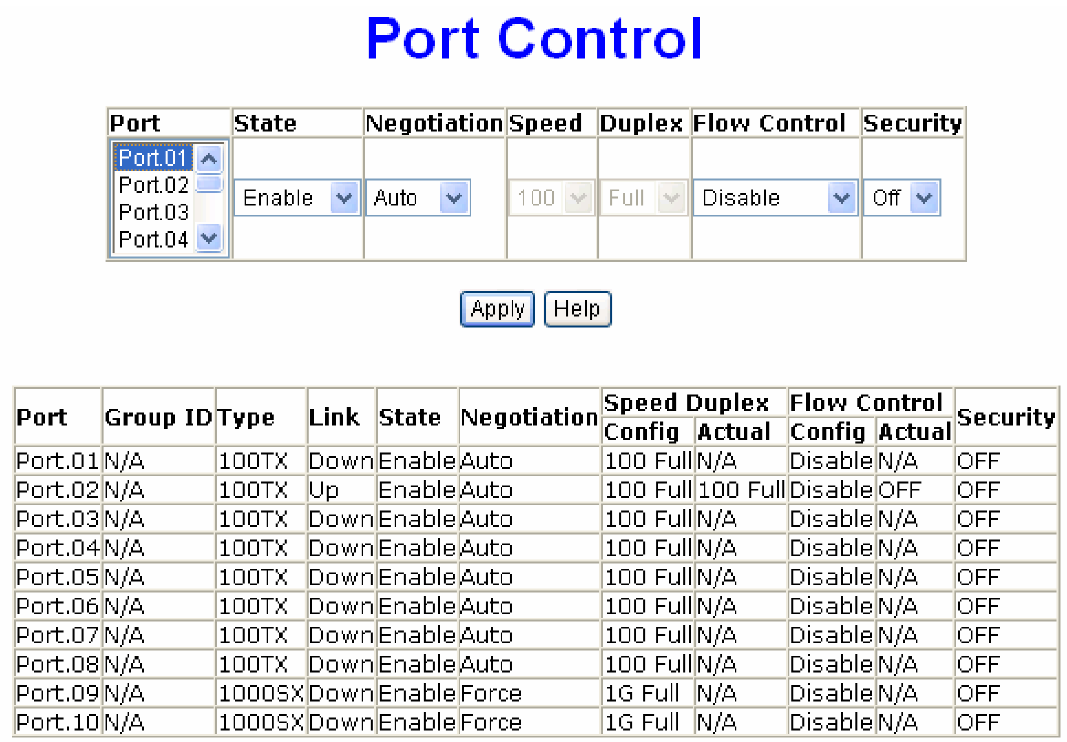
Port Statistics interface

Port Control

In Port control, you can view the parameters of the ports.

1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be disabled or enabled. If the port setting is disabled then will not receive or transmit any packet.

3. **Negotiation:** set auto negotiation status of the port.
4. **Speed:** set the port link speed. TX can 10/100, FX is always 100
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set the flow control function as **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Disable**.
7. **Security:** When its state is "**On**", means this port accepts only one MAC address.
8. Click Apply .



Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.03 Port.04	Enable	Auto	100	Full	Disable	Off

Apply Help

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.02	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Disable	OFF	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Disable	N/A	OFF
Port.09	N/A	1000SX	Down	Enable	Force	1G Full	N/A	Disable	N/A	OFF
Port.10	N/A	1000SX	Down	Enable	Force	1G Full	N/A	Disable	N/A	OFF

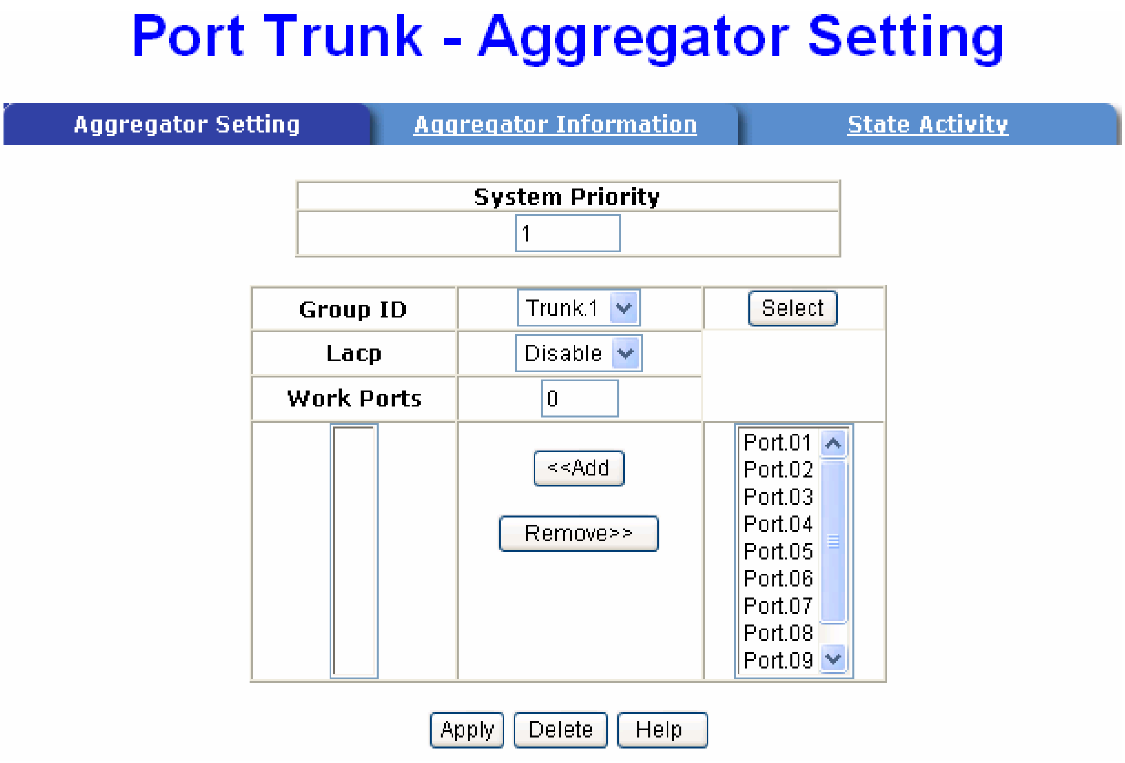
Port Control interface

Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to seven consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detailed information refers to IEEE 802.3ad.

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are three trunk groups to provide configure. Choose the "**Group ID**" and click Select.
3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. **Work ports:** allows maximum of four ports that can be aggregated at the same time. With LACP static trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is a local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to join the trunk group. Allows four ports maximum that can be aggregated at the same time. Click the Add button to add the port. To remove unwanted ports, select the port and click the Remove button.
6. If LACP is enabled, you can configure the LACP Active/Passive status in each port on the State Activity page.
7. Click Apply.
8. Use the Delete button to delete the Trunk Group. Select the Group ID and click Delete button.



Port Trunk - Aggregator Setting

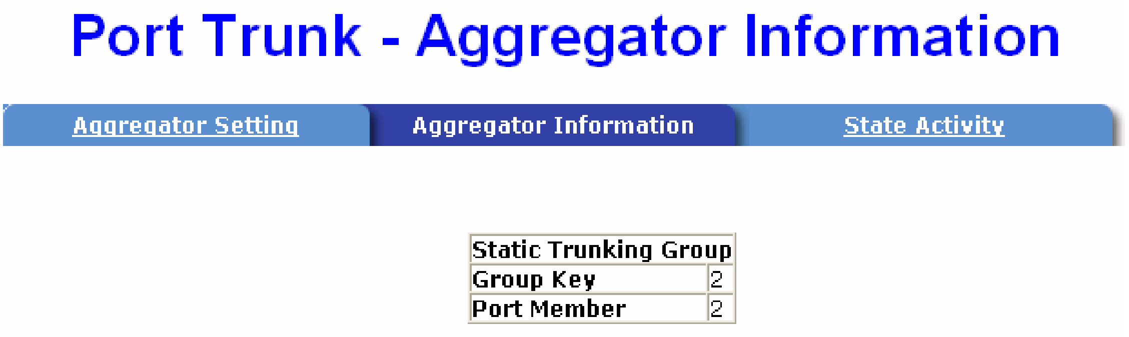
System Priority: 1

Group ID	Trunk.1	Select
Lacp	Disable	
Work Ports	0	

Port Trunk—Aggregator Setting interface

Aggregator Information

When setting up the LACP aggregator, you will see the relation information here.



Port Trunk - Aggregator Information

Static Trunking Group	
Group Key	2
Port Member	2

Port Trunk – Aggregator Information interface

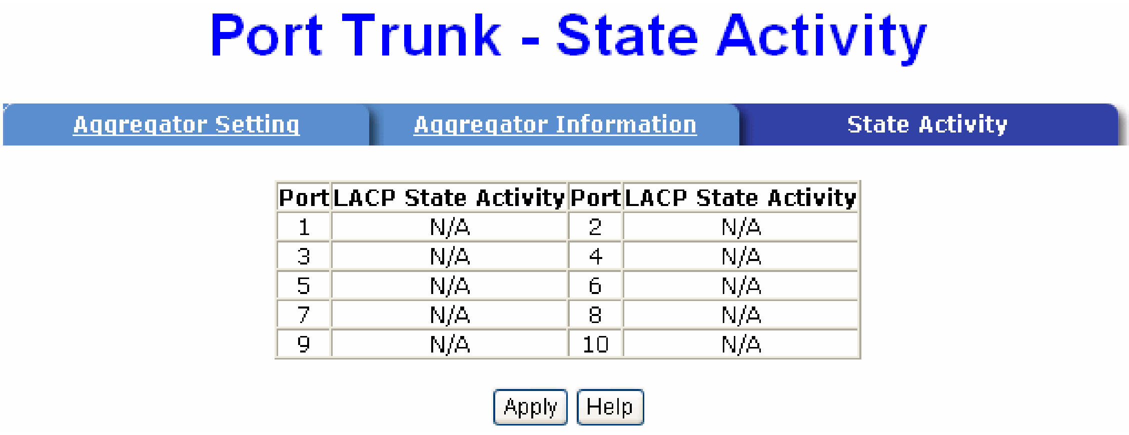
State Activity

After setting up the LACP aggregator, you can configure the port state activity. You can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to **Active**. Opposite is **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. A link having either two active LACP ports or one active port can perform as a dynamic LACP trunk.
2. A link has two passive LACP ports will not perform as a dynamic LACP trunk because both ports are waiting for the LACP protocol packet from the opposite device.
3. If you are an active LACP, after you have selected trunk port, the active status will be created automatically.



Port	LACP State Activity	Port	LACP State Activity
1	N/A	2	N/A
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A

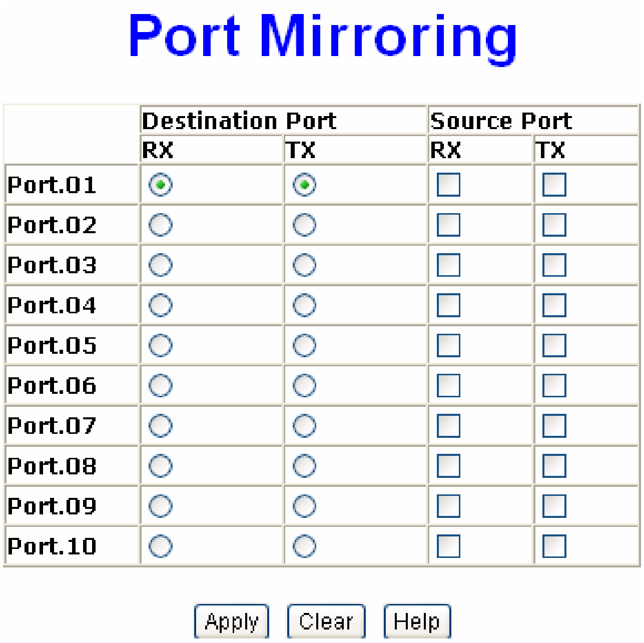
Port Trunk – State Activity interface

Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. Traffic goes in or out monitored (source) ports will be duplicated into a mirrored (destination) port.

- **Destination Port:** There is only one port can be selected to be a destination (mirrored) port for monitoring both RX and TX traffic which comes from the source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. The user can connect the mirrored port to a LAN analyzer.

- **Source Port:** The ports that the user wants to monitor. All monitored port traffic will be copied to the mirrored (destination) port. The user can select multiple source ports by checking the **RX** or **TX** check boxes to be monitored.
- And then, click Apply button.



Port Mirroring

	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	●	●	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□
Port.05	○	○	□	□
Port.06	○	○	□	□
Port.07	○	○	□	□
Port.08	○	○	□	□
Port.09	○	○	□	□
Port.10	○	○	□	□

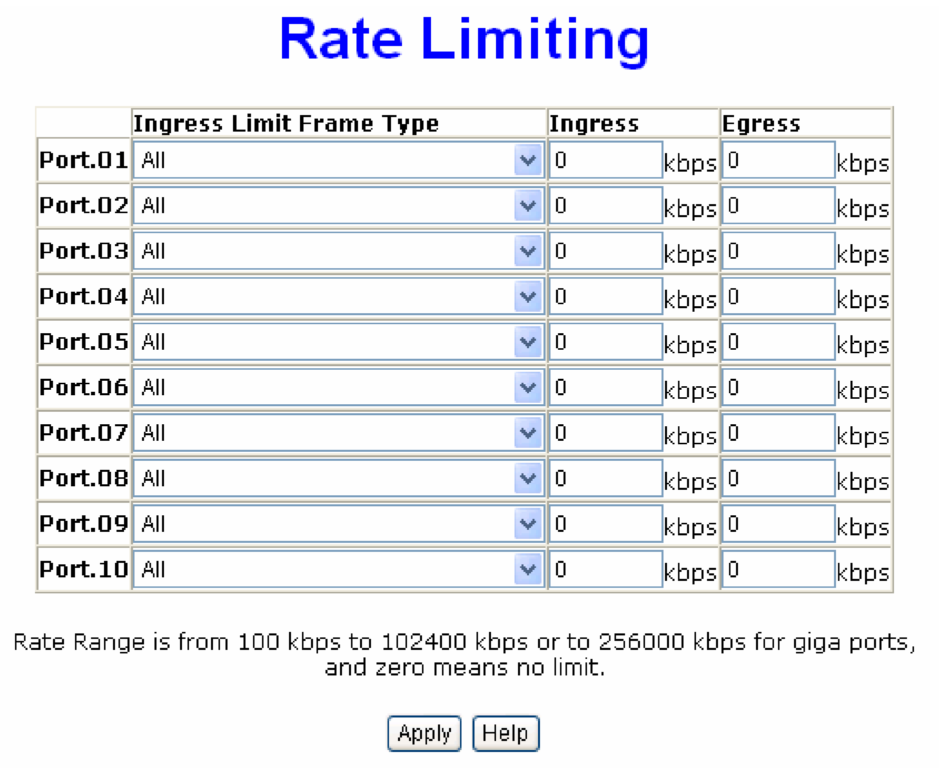
Port Trunk – Port Mirroring interface

Rate Limiting

You can set up the bandwidth rate and frame limitation type for each port.

- **Ingress Limit Frame type:** select the frame type that is to be filtered. The frame types have 4 filtering options: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast** and **Broadcast only**.

  Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Broadcast only** types are only for ingress frames. The egress rate supports **All** types.



Rate Limiting

	Ingress Limit Frame Type	Ingress		Egress	
Port.01	All	0	kbps	0	kbps
Port.02	All	0	kbps	0	kbps
Port.03	All	0	kbps	0	kbps
Port.04	All	0	kbps	0	kbps
Port.05	All	0	kbps	0	kbps
Port.06	All	0	kbps	0	kbps
Port.07	All	0	kbps	0	kbps
Port.08	All	0	kbps	0	kbps
Port.09	All	0	kbps	0	kbps
Port.10	All	0	kbps	0	kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate to 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate
  - **Ingress:** Enter the port effective ingress rate (The default value is "0")
  - **Egress:** Enter the port effective egress rate (The default value is "0")
- And then, click Apply to apply the settings

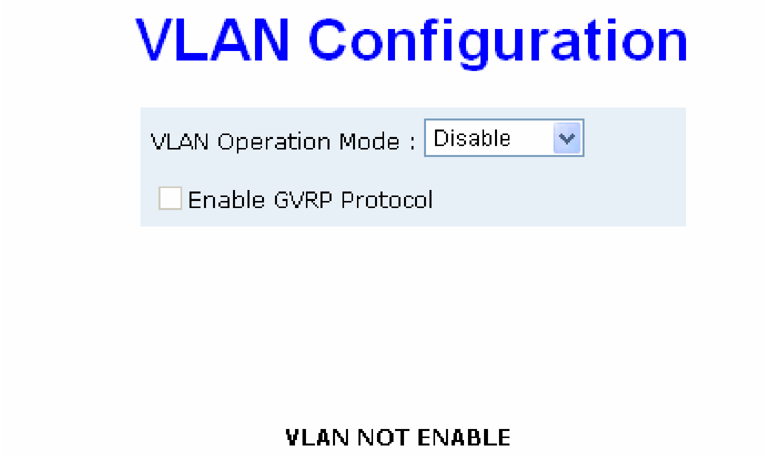
[NOTE] Rate Range is from 64 kbps to 102400 kbps (250000 kbps for giga ports) and zero means no limit

---

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would, allow you to isolate network traffic so only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The industrial switch supports port-based and 802.1Q (tagged-based) VLANs. In the default configuration, the VLAN operation default mode is “**Disable**”.



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protocol

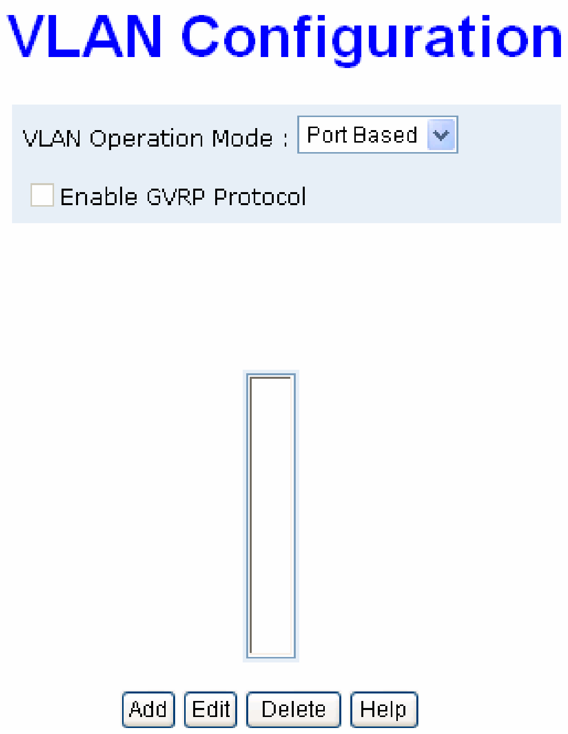
VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration - Port-based VLAN

Packets can only travel among members of the same VLAN group. All unselected ports (not belonging to a specified VLAN group) are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware ‘bridge’ that is capable of classifying and tagging the packet with different VLAN IDs based on not only default PVIDs but also with other information about the packet, such as the protocol.



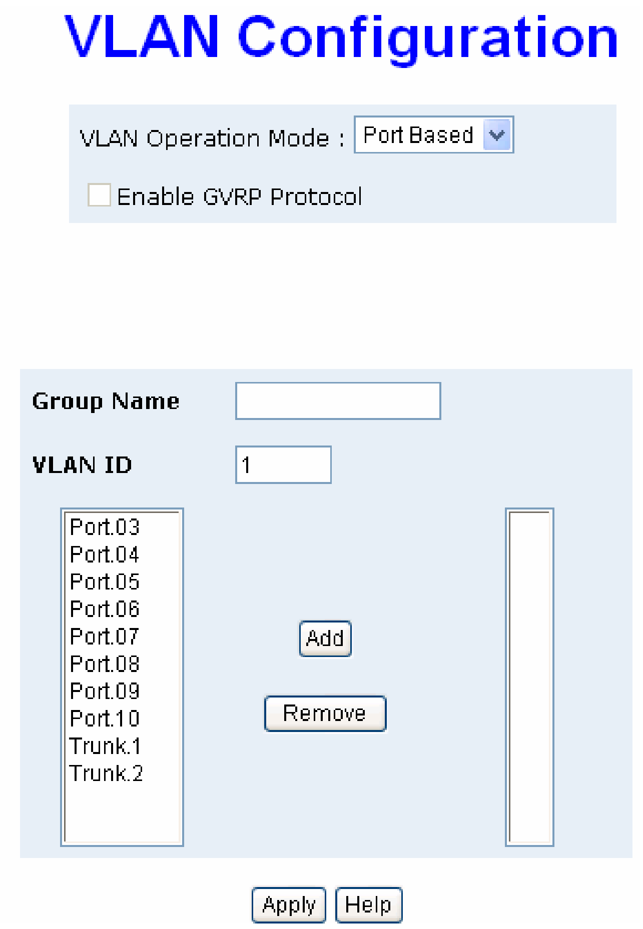
VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

VLAN – Port Based interface

- Click Add to add a new VLAN group (The maximum number of VLAN groups is 64)
- Enter the VLAN name, group ID and port numbers of the VLAN group
- Click Apply



VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Group Name

VLAN ID 1

Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10
Trunk.1
Trunk.2

VLAN—Port Based Add interface

- You will see the VLAN displayed.
- Use the Delete button to delete the unwanted VLAN.
- Use the Edit button to modify an existing VLAN group.

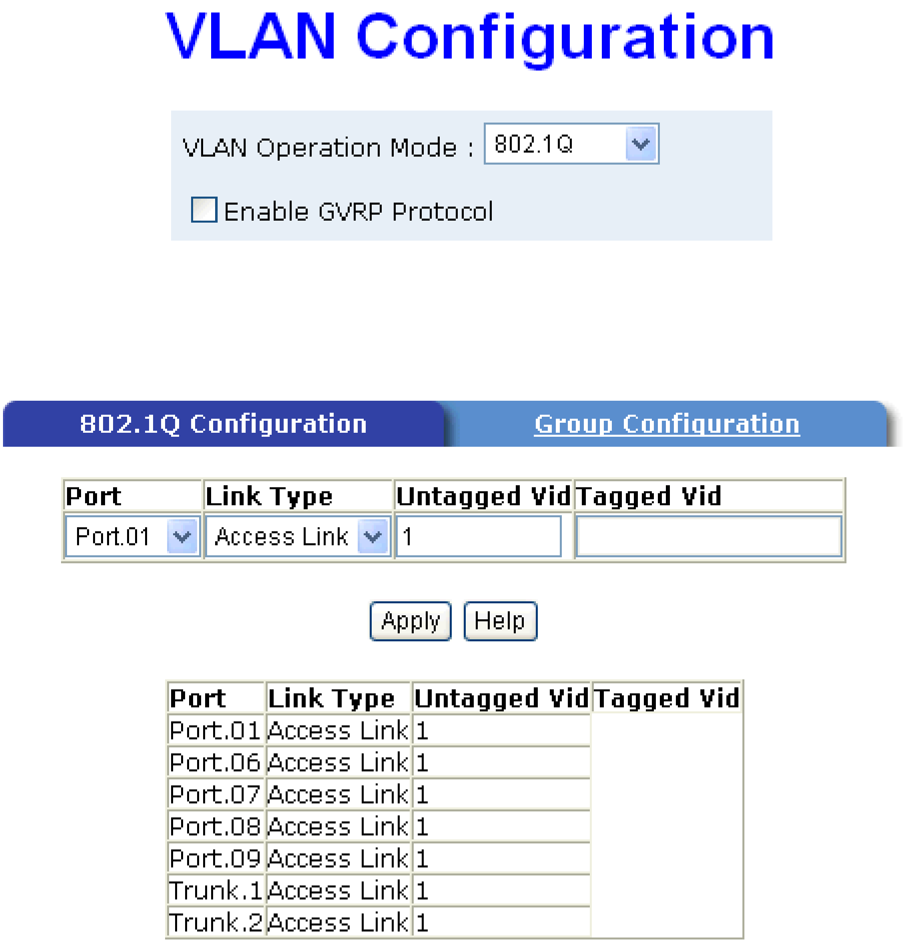
[NOTE] Remember to execute the "Save Configuration" action, otherwise the new configuration will be lost when switch power is powered down.

802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. The tag contains a VLAN Identifier (VID) that indicates the VLAN information.

You can create a Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups available. To enable an 802.1Q VLAN, all the ports on the switch belong to the default VLAN; the VID is 1. The default VLAN cannot be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Trunk.1	Access Link	1	
Trunk.2	Access Link	1	

802.1q VLAN interface

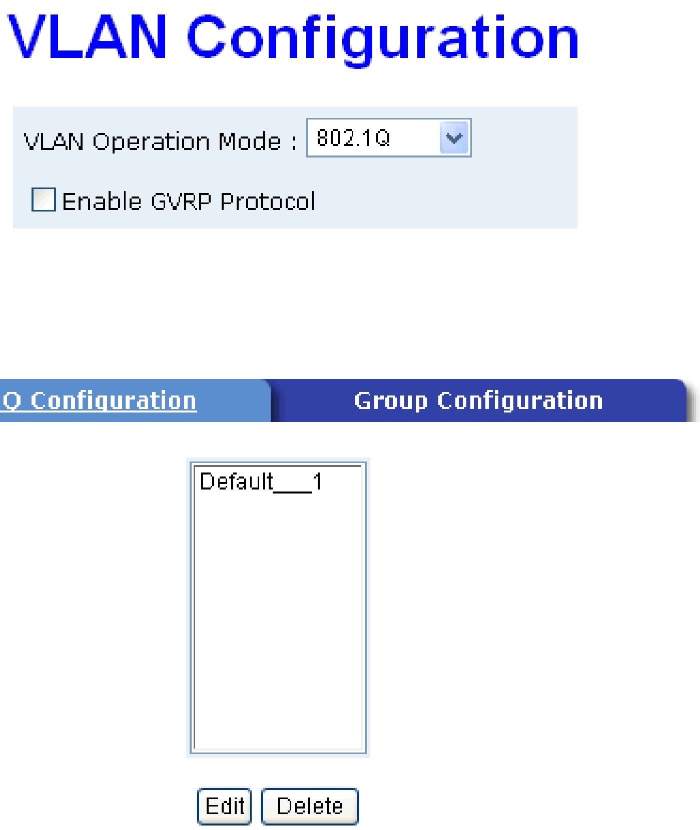
802.1Q Configuration

1. To **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that you want to configure.
3. **Link Type**: there are 3 link types.
   - **Access Link:** single switch only, allows user to group ports by setting the same VID.
   - **Trunk Link:** extended application of **Access Link**, allows user to group ports by setting the same VID with 2 or more switches.
   - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame a VID.
5. **Tagged VID:** assign the tagged frame a VID.
6. Click Apply
7. You can see each port setting in the table on the screen.

Group Configuration

Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click Apply


VLAN Configuration

VLAN Operation Mode : 802.1Q

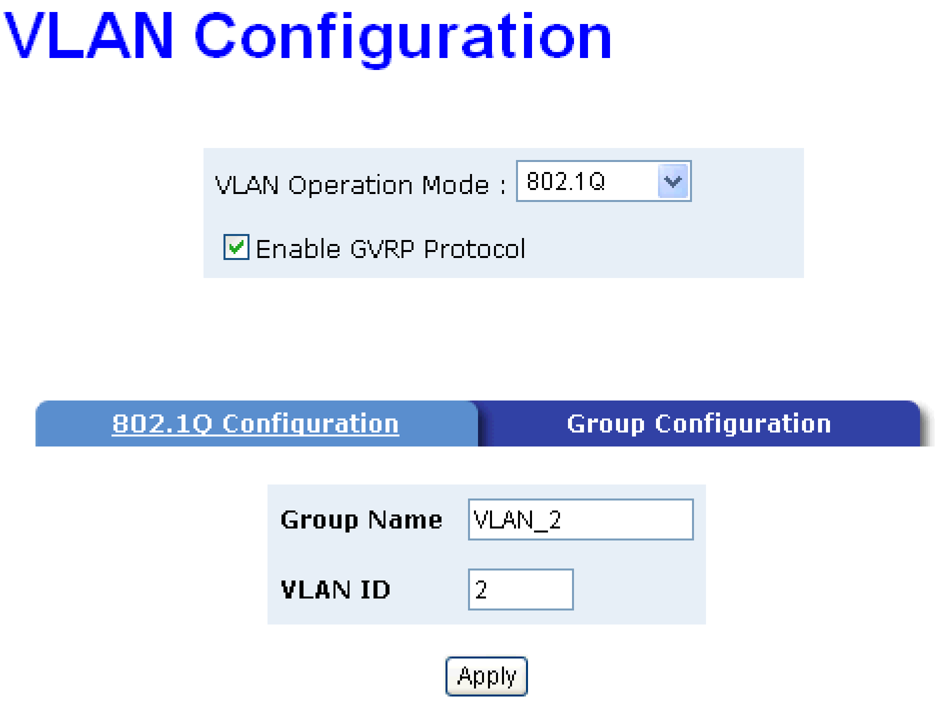
□ Enable GVRP Protocol

Default___1

Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.

4. Click Apply.


VLAN Configuration

VLAN Operation Mode : 802.1Q

☑ Enable GVRP Protocol

Group Name: VLAN_2

VLAN ID: 2

Group Configuration interface

Rapid Spanning Tree

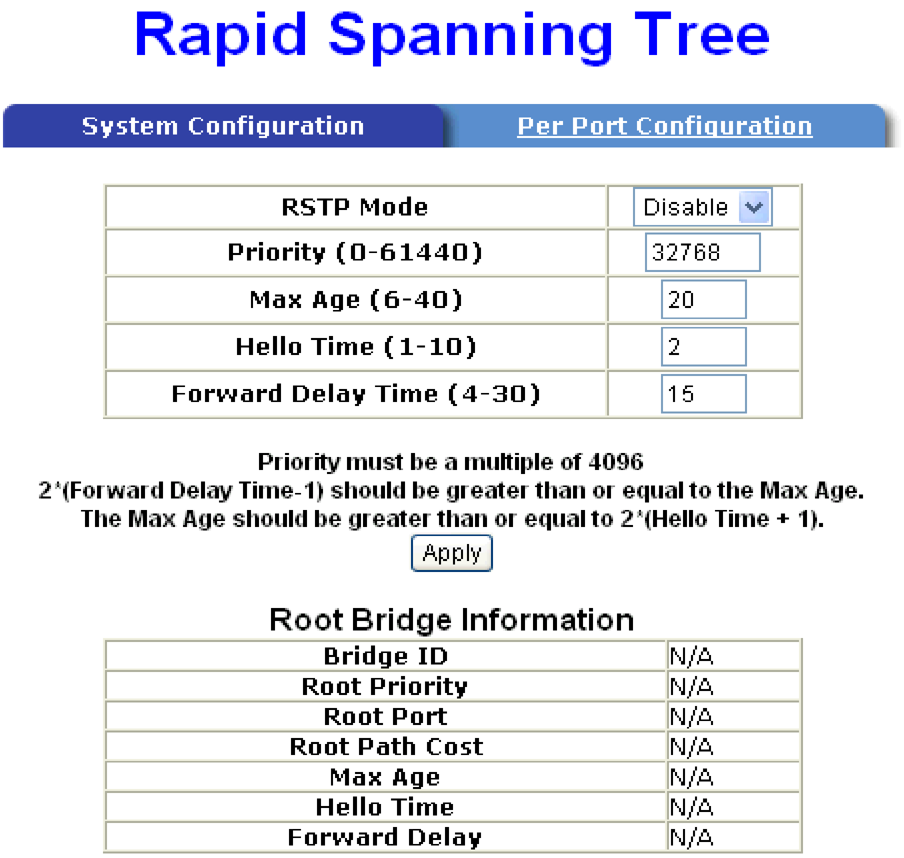
The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

RSTP System Configuration

- The user can view the spanning tree information about the Root Bridge
- User can modify the RSTP state. After modification, click the Apply button
  - **RSTP mode:** user must enable or disable the RSTP function before configuring the related parameters
  - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule
  - **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
  - **Hello Time (1-10):** the time that before a switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
  - **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

[NOTE] Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)



Rapid Spanning Tree

RSTP Mode	Disable
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Root Bridge Information

Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age	N/A
Hello Time	N/A
Forward Delay	N/A

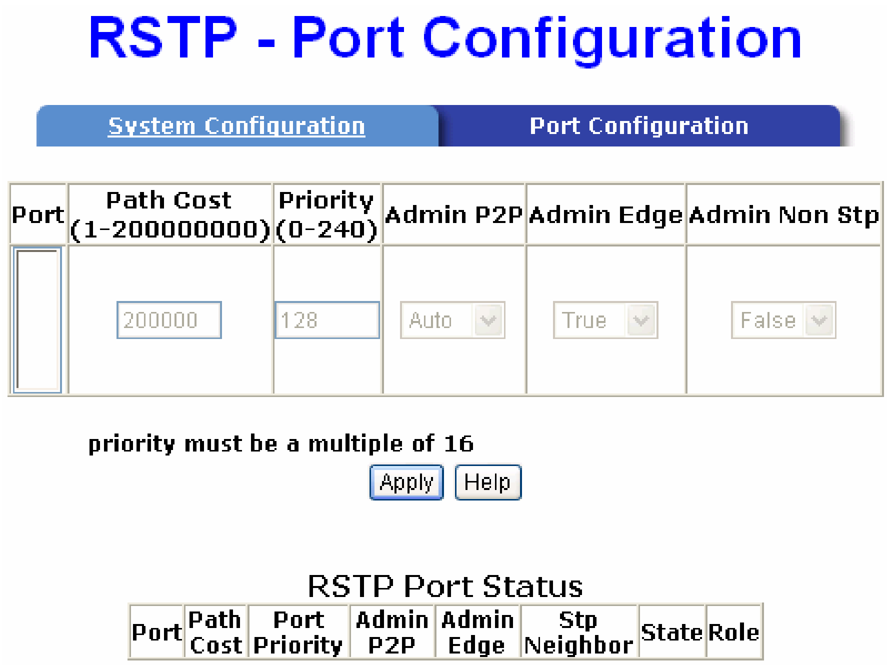
RSTP System Configuration interface

RSTP Port Configuration

You can configure the path cost and priority of every port.

8. Select the port in the Port column.
1. **Path Cost:** The cost of the path to the other bridge from the transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
2. **Priority:** Decide which port should be blocked by priority in the LAN. Enter a number 0 through 240. The value of the priority must be the multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
4. **Edge:** The port directly connected to end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to “**True**” status.

5. **Non Stp:** The port includes the STP mathematic calculation. **True** is not including the STP mathematic calculation. **False** is including the STP mathematic calculation.
6. Click Apply.



RSTP - Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
	200000	128	Auto	True	False

priority must be a multiple of 16

RSTP Port Status

Port	Path Cost	Port Priority	Admin P2P	Admin Edge	Stp Neighbor	State	Role

RSTP Per Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

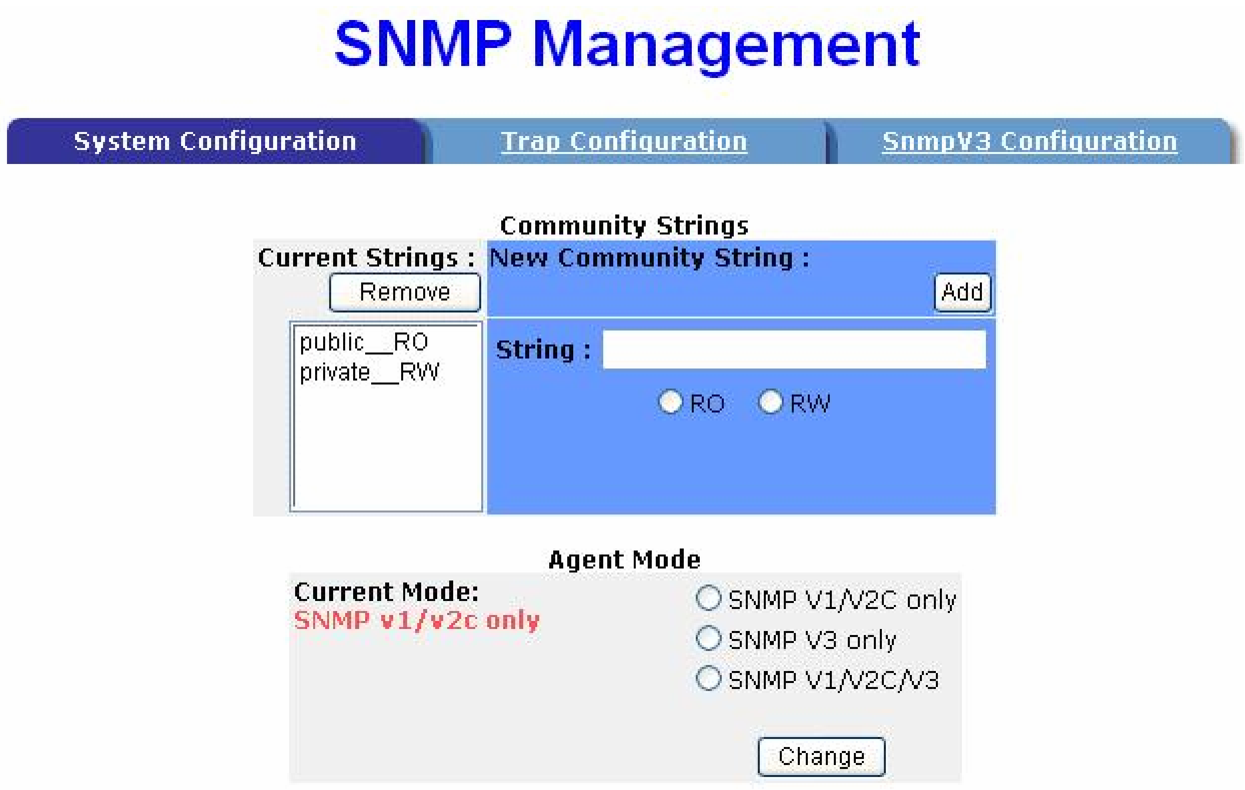
System Configuration

- **Community Strings**

You can define a new community string set and remove an unwanted community string.

1. **String:** Type the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use . Click Change to switch to the selected SNMP version mode.



Community Strings

Current Strings : Remove

public__RO
private__RW

New Community String : Add

String :

○ RO ○ RW

Agent Mode

Current Mode:
SNMP v1/v2c only

○ SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

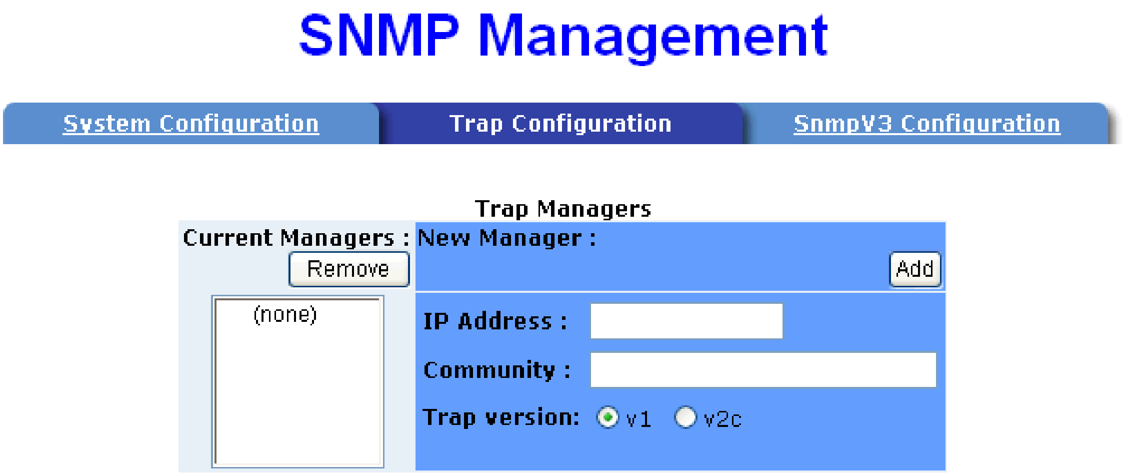
Change

SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives traps and the system alerts generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap managers, enter the SNMP community strings and select the SNMP version.

1. **IP Address:** enter the IP address of trap manager.
2. **Community:** enter the community string.
3. **Trap Version:** select the SNMP trap version type – v1 or v2.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot remove the default community string set.



SNMP Management

System Configuration | Trap Configuration | SnmpV3 Configuration

Trap Managers

Current Managers : Remove

(none)

New Manager : Add

IP Address :

Community :

Trap version: ● v1 ○ v2c

Trap Managers interface

SNMP V3 Configuration

Configure the SNMP V3 function.

Context Table

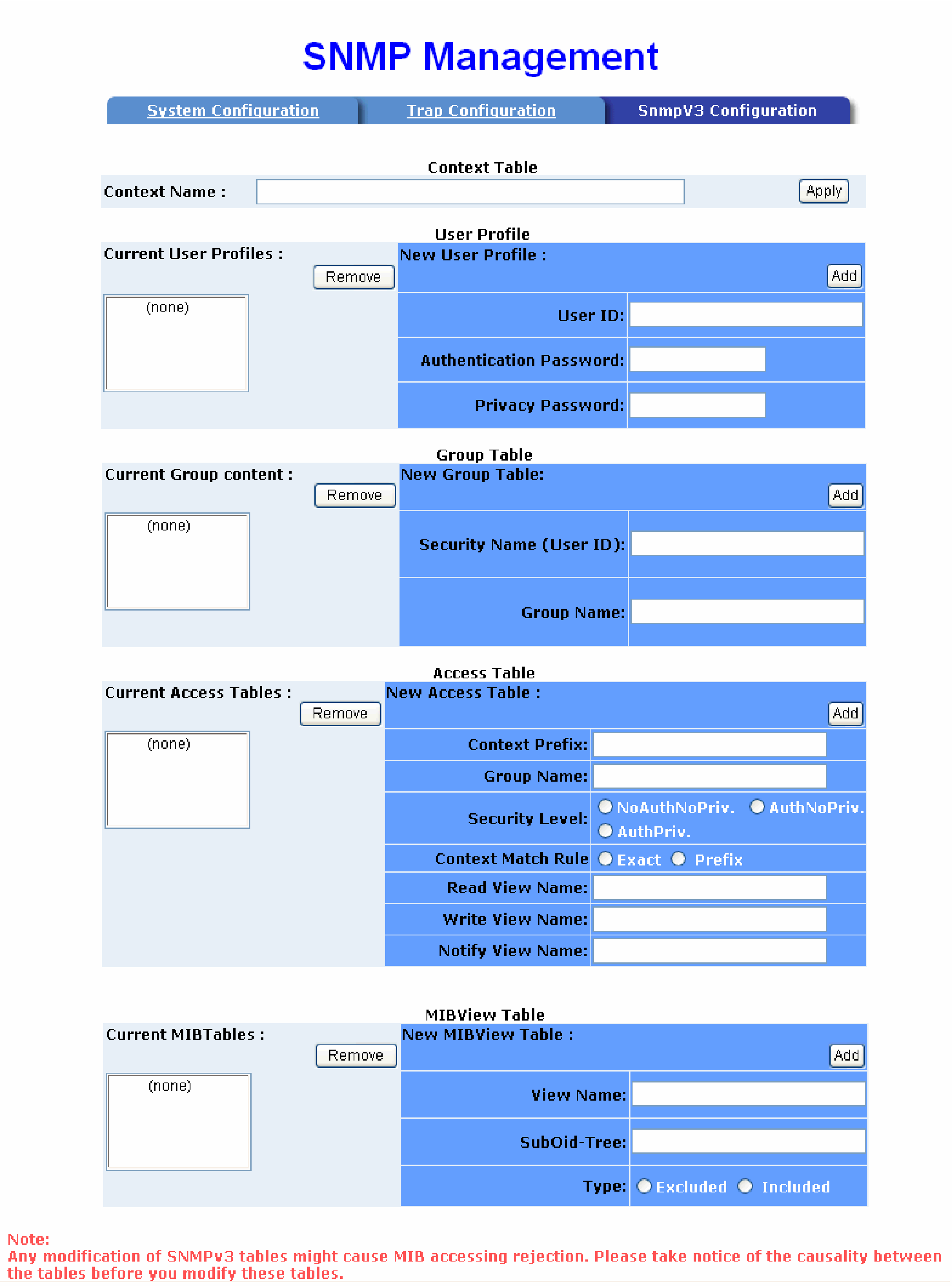
To configure SNMP v3 context table, assign the context name of the context table. Click Add to add the context name. Click Remove to remove an unwanted context name.

User Profile

To configure the SNMP v3 user table

- **User ID:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Click Add to add context name.

Click Remove to remove an unwanted context name.



SNMP Management

System Configuration | Trap Configuration | SnmpV3 Configuration

Context Table

Context Name : [ ] Apply

User Profile

Current User Profiles : Remove

(none)

New User Profile : Add

User ID: [ ]

Authentication Password: [ ]

Privacy Password: [ ]

Group Table

Current Group content : Remove

(none)

New Group Table: Add

Security Name (User ID): [ ]

Group Name: [ ]

Access Table

Current Access Tables : Remove

(none)

New Access Table : Add

Context Prefix: [ ]

Group Name: [ ]

Security Level: ○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.

Context Match Rule ○ Exact ○ Prefix

Read View Name: [ ]

Write View Name: [ ]

Notify View Name: [ ]

MIBView Table

Current MIBTables : Remove

(none)

New MIBView Table : Add

View Name: [ ]

SubOid-Tree: [ ]

Type: ○ Excluded ○ Included

Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

SNMP V3 configuration interface

Group Table

To configure an SNMP v3 group table.

- **Security Name (User ID):** assign the user name that you have set up in user table.
- **Group Name:** set up the group name.

- Click Add to add the context name.
- Click Remove to remove an unwanted context name.

Access Table

To configure the SNMP v3 access table.

- **Context Prefix:** set up the context name.
- **Group Name:** set up the group.
- **Security Level:** select the access level.
- **Context Match Rule:** select the context match rule.
- **Read View Name:** set up the read view.
- **Write View Name:** set up the write view.
- **Notify View Name:** set up the notify view.
- Click Add to add context name.
- Click Remove to remove an unwanted context name.

MIB view Table

To configure a MIB view table.

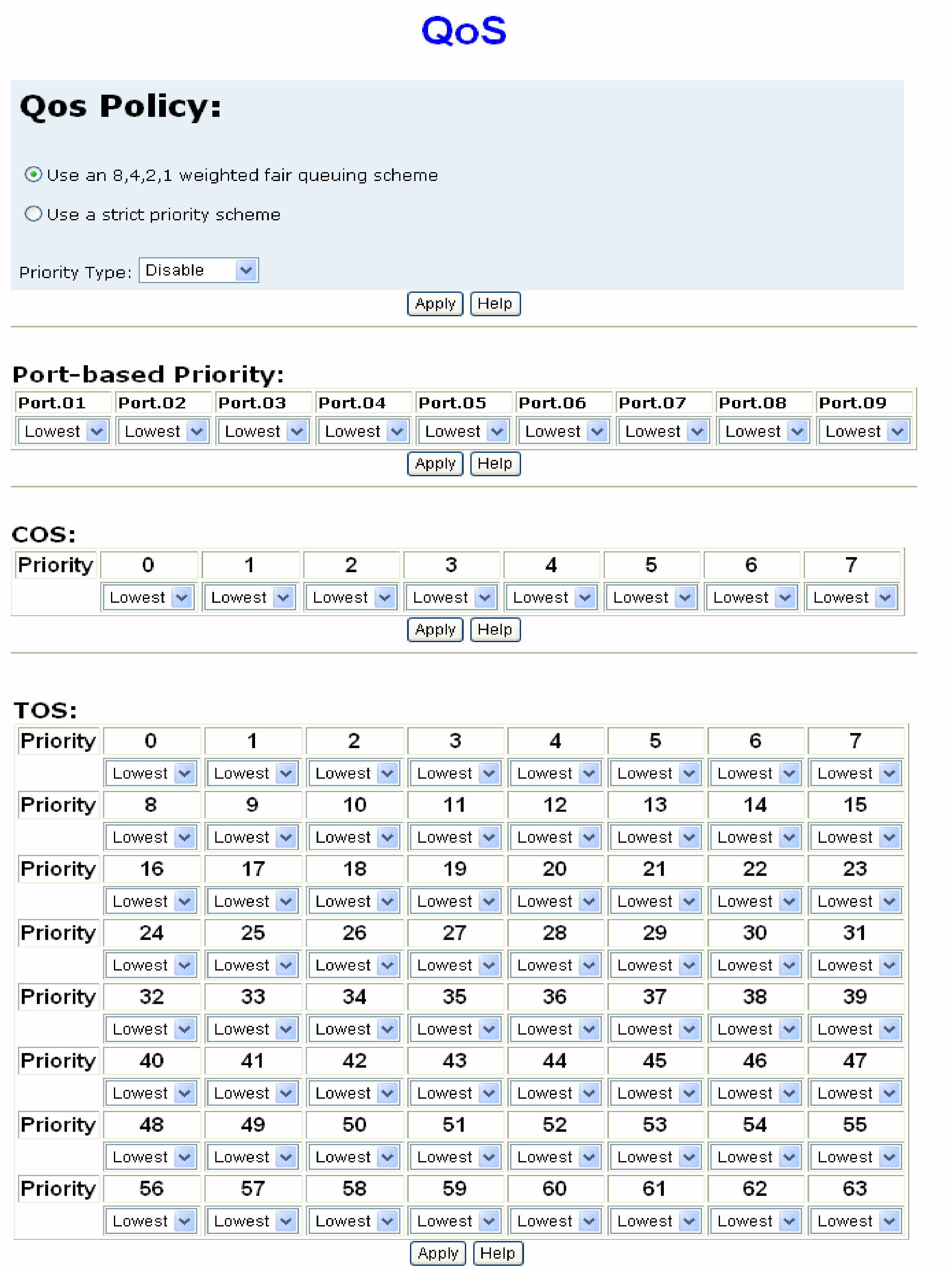
- **ViewName:** set up the name.
- **Sub-Oid Tree:** fill the Sub OID.
- **Type:** select the type – exclude or included.
- Click Add to add a context name.
- Click Remove to remove an unwanted context name.

QoS Configuration

You can configure QoS policy and priority setting, per port priority setting, and the COS and TOS settings.

QoS Policy and Priority Type

- **Qos Policy:** select the QoS policy rule.
    - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from Hi to lowest queue. For example: the system will process 80 % high queue traffic, 40 % middle queue traffic, 20 % low queue traffic, and 10 % lowest queue traffic at the same time. And the traffic in the Low Priority queue is not transmitted until all High, Medium, and Normal traffic are serviced.
    - **Use the strict priority scheme:** The higher queue will always be processed first, except when the higher queue is empty.
- **Priority Type:** there are 5 priority type selections available. Disable means no priority type is selected.
- **Port-base:** the port priority will follow the **Port-base** that you have assigned – High, middle, low, or lowest.
    - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
    - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
    - **COS first:** the port priority will follow the COS priority first, and then other priority rules.
    - **TOS first:** the port priority will follow the TOS priority first, and the other priority rules.
- Click Apply .



QoS

Qos Policy:

● Use an 8,4,2,1 weighted fair queuing scheme

○ Use a strict priority scheme

Priority Type: Disable

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08	Port.09
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

COS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

TOS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	8	9	10	11	12	13	14	15
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	16	17	18	19	20	21	22	23
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	24	25	26	27	28	29	30	31
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	32	33	34	35	36	37	38	39
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	40	41	42	43	44	45	46	47
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	48	49	50	51	52	53	54	55
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	56	57	58	59	60	61	62	63
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

QoS Configuration interface

Port Based Priority

To configure port priority levels.

- **Port 1 ~ Port 10:** each port has 4 priority levels – High, Middle, Low, and Lowest.

- Click Apply.

COS Configuration

To set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

To set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority levels. Each level has 4 types of priority – high, middle, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that it has received. For example: the user sets the TOS level to 25 (high). The port 1 is following the TOS priority policy only. When the port 1 packet is received, the system will check the TOS value of the received IP packet. If the TOS value of the received IP packet is 25 (priority = high), then the packet priority will have highest priority.
- Click Apply.

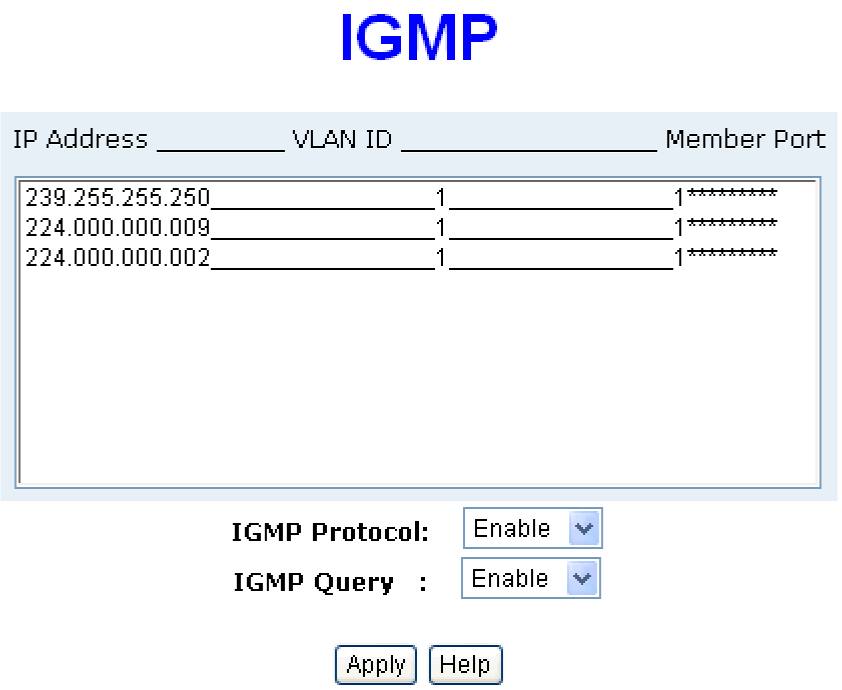
IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and to report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of messages:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

If the switch supports IP multicast, you can enable IGMP protocol on the web management switch setting advanced page, then display the IGMP snooping information. IP multicast addresses range from 224.0.0.0 to 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be displayed in the IGMP status section.
- Click Apply.



IGMP

```
IP Address __________ VLAN ID ____________________ Member Port

239.255.255.250____________________1____________________1*********
224.000.000.009____________________1____________________1*********
224.000.000.002____________________1____________________1*********
```

IGMP Protocol: Enable

IGMP Query : Enable

X-Ring Redundancy

X-Ring Redundancy provides a faster redundant recovery scheme than the Rapid Spanning Tree scheme. The action is similar to STP or RSTP, but the algorithms are not the same, and the amount of cabling simpler.

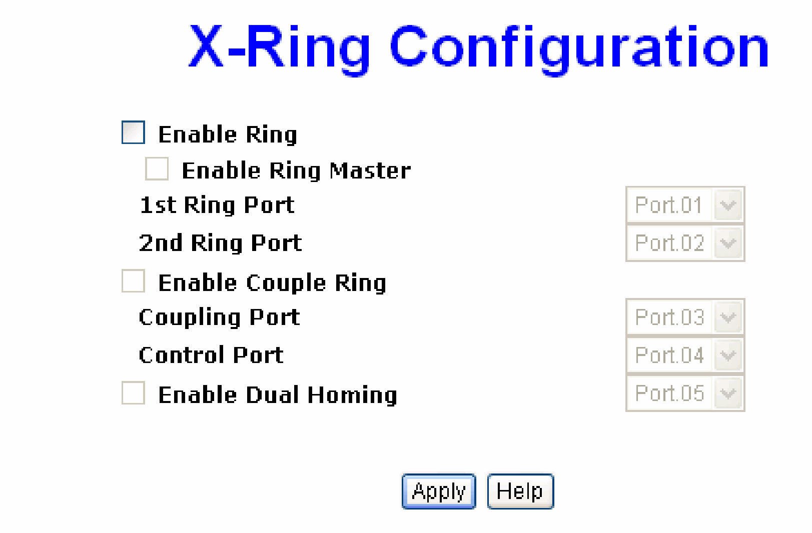
In the X-Ring topology, every switch should enable the X-Ring function and assign two member ports for the ring. Only one switch in the X-Ring group would be set as a Ring Master switch. Other switches are called working switches and their two member ports are called working ports. When the failure of a network connection occurs in the ring, the Ring Master will automatically transmit the packets over the remaining member port.

The ring master can negotiate and send commands to other switches in the X-Ring group. If there are 2 or more switches in master mode, then the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, the user can identify the switch as the ring master from the R.M. LED of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring groups for the redundant backup function and dual homing function that prevents connection loss between X-Ring groups and upper level/core switches.

- **Enable X-Ring:** To enable the X-Ring function. Mark the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box for enabling this switch to be the ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- **Enable Coupling Ring:** To enable the coupling ring function, mark the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port.

- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. In an X-Ring group, only one port can be the Dual Homing port. Dual Homing only works when the X-Ring function is enabled.
- Click Apply to apply the configuration.



X-Ring Configuration

□ Enable Ring

□ Enable Ring Master

1st Ring Port: Port.01

2nd Ring Port: Port.02

□ Enable Couple Ring

Coupling Port: Port.03

Control Port: Port.04

□ Enable Dual Homing: Port.05

X-ring Interface

[NOTE]

1. When the X-Ring function is enabled, the user must disable RSTP. The X-Ring function and the RSTP function cannot exist at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when the switch is powered down.

Security

In this section, you can configure 802.1x and MAC address table.

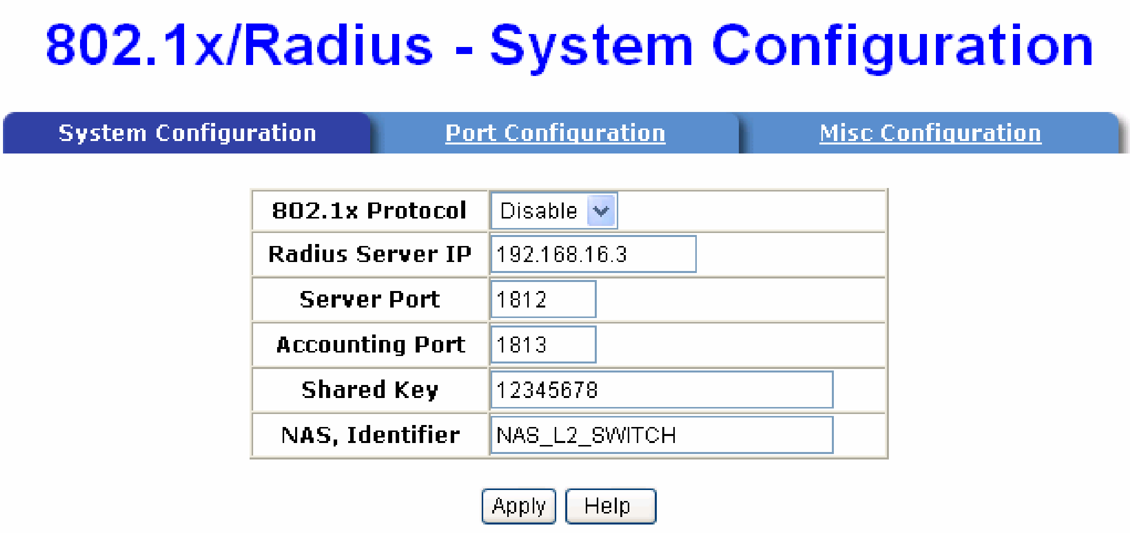
802.1X/Radius Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Click Apply.



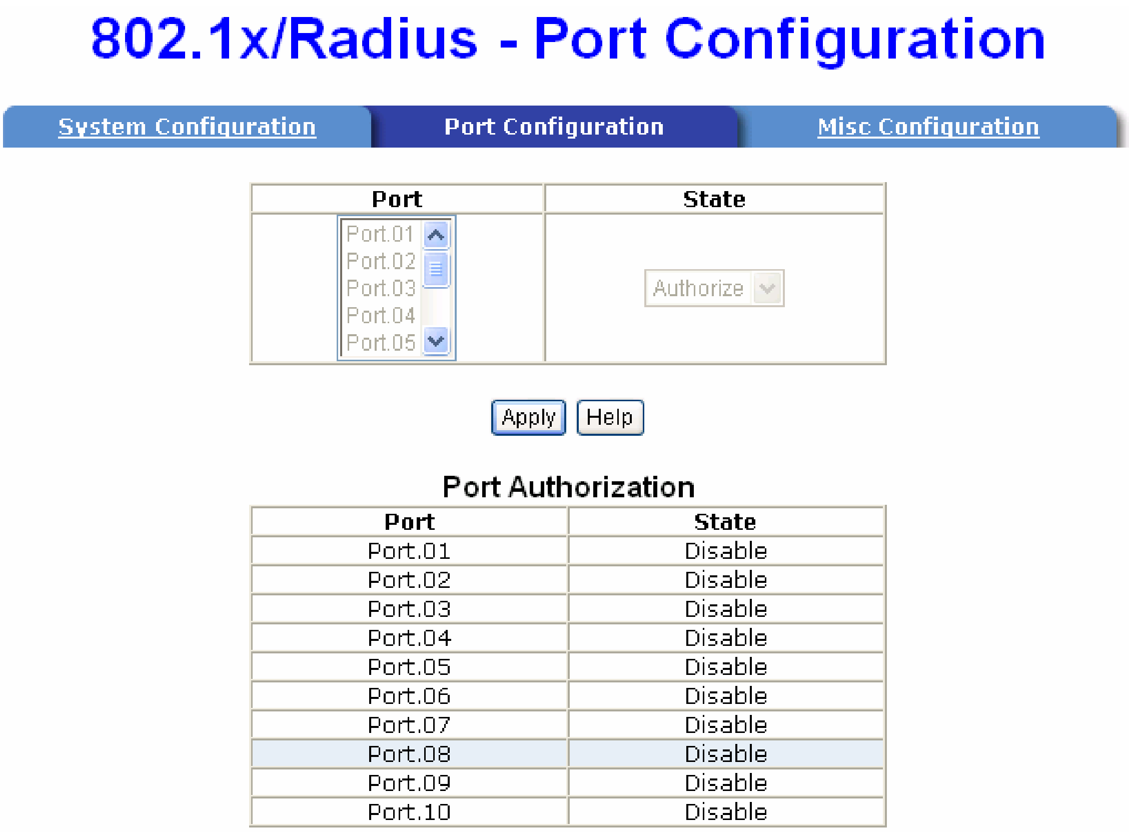
802.1x Protocol	Disable
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

802.1x System Configuration interface

802.1x Port Configuration

You can configure the 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use the “**Space**” key to change the state value.

- **Reject:** the specified port is required to be held in the Unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Click Apply.



Port Authorization

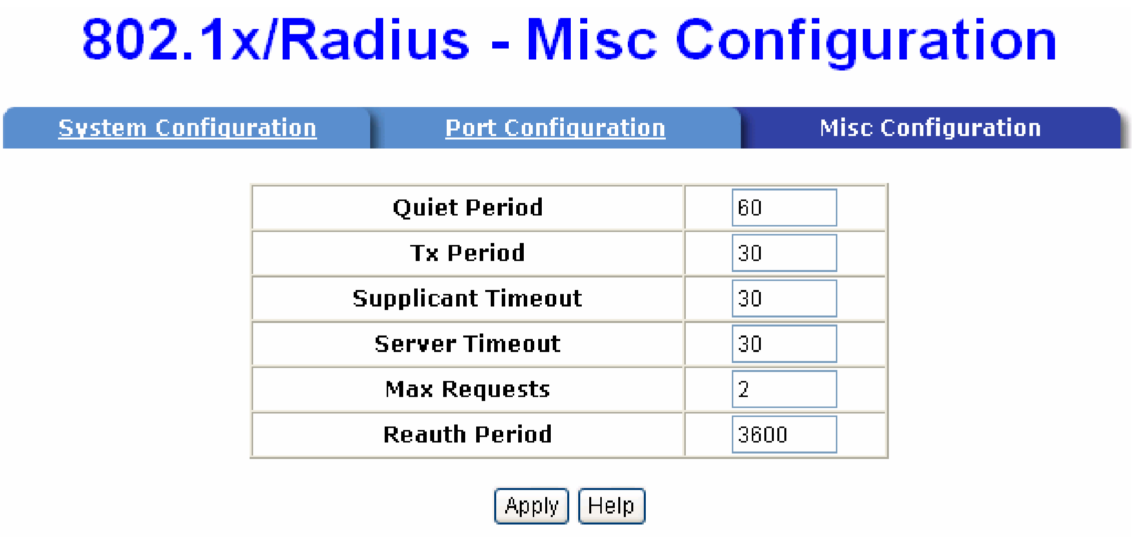
Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable

802.1x Per Port Setting interface

Miscellaneous Configuration

1. **Quiet Period:** set the period during which the port does not try to acquire a supplicant.

2. **TX Period:** set the period for the port wait to re-transmit the next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentications that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which connected clients must be re-authenticated.
7. Click Apply.



802.1x/Radius - Misc Configuration

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure port security.

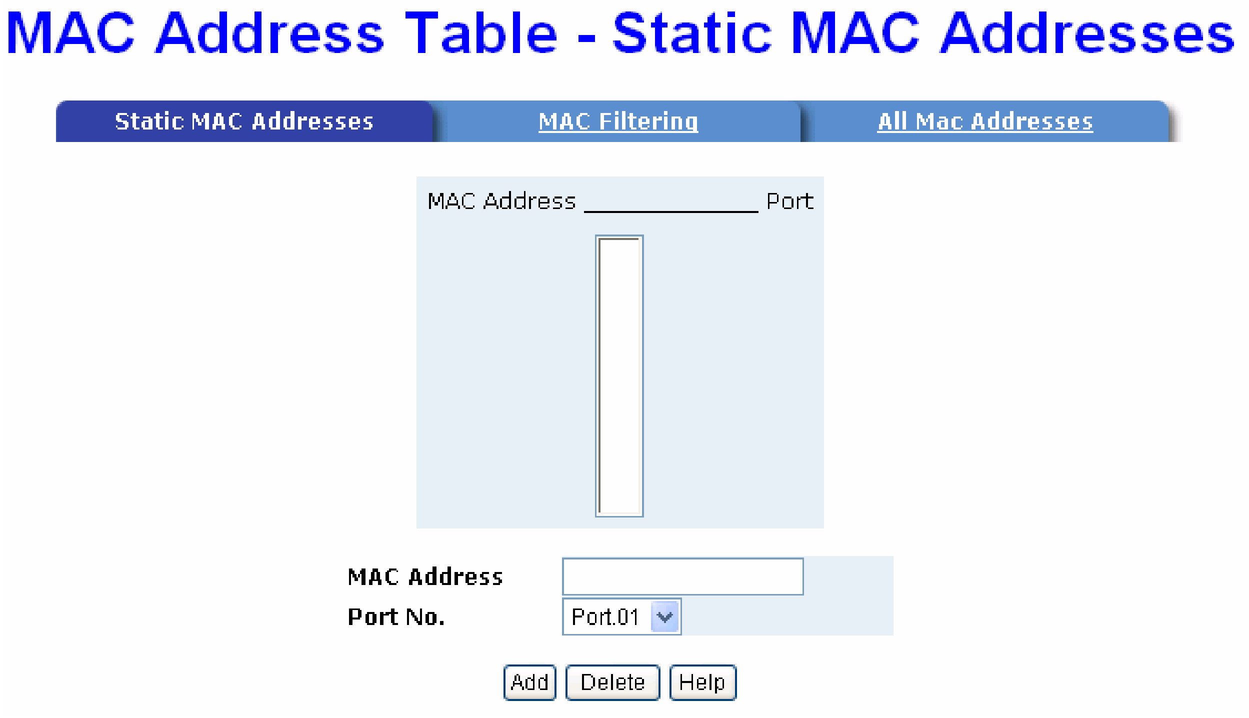
Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

- **Add the Static MAC Address**

You can add static MAC address in the switch MAC table.

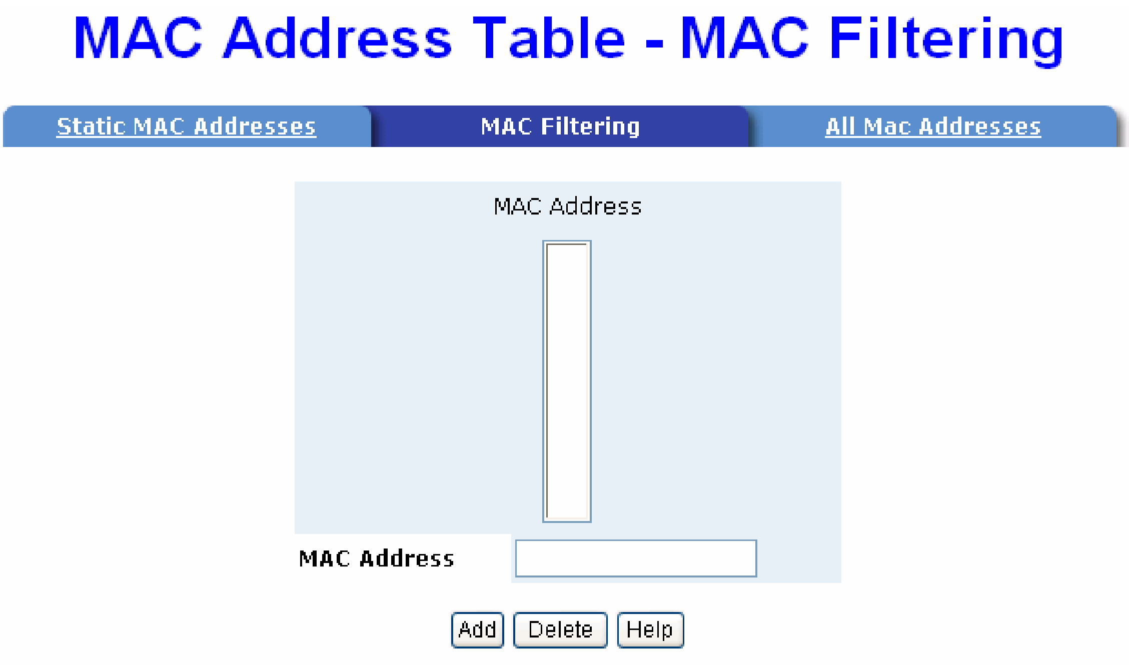
1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device's network activity.
2. **Port No.:** pull down the selection menu to select the port number.
3. Click Add.
4. If you want to delete the MAC address from the filtering table, select the MAC address and click Delete.



Static MAC Addresses interface

MAC Filtering

By filtering MAC addresses, the switch can easily filter pre-configured MAC addresses and enhance security. You can add and delete the filtering MAC address.



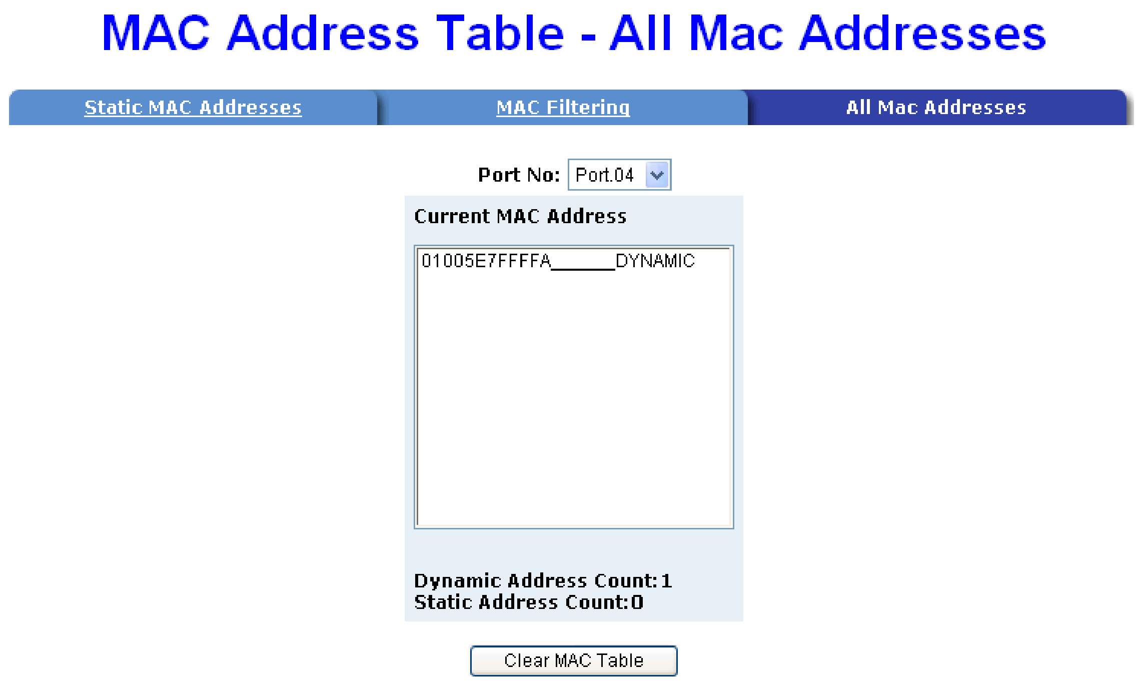
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. Click Add.
3. If you want to delete the MAC addresses from the filtering table, select the MAC address and click Delete.

All MAC Addresses

You can view the port that is connected to the device’s MAC address and related devices’ MAC addresses.

1. Select the port.
2. The selected port of the static MAC address information will be displayed.
3. Click Clear MAC Table to clear the current port static MAC address information on the screen.



Port No: Port.04

Current MAC Address

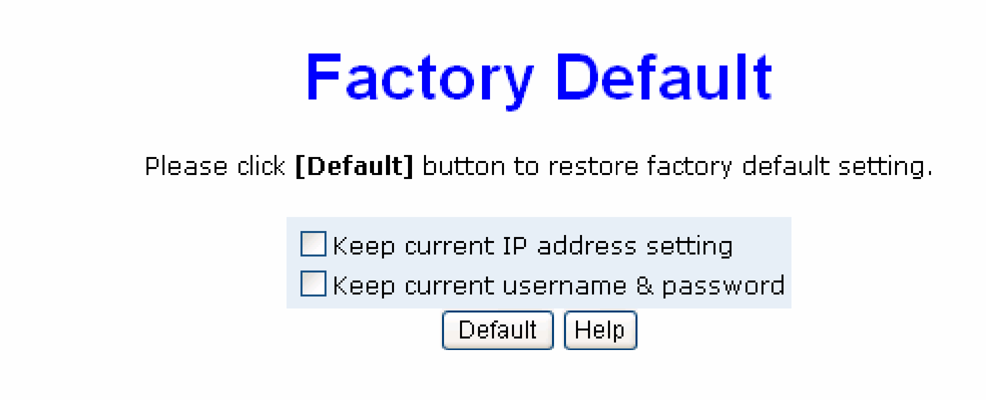
```
01005E7FFFFA______DYNAMIC
```

Dynamic Address Count:1
Static Address Count:0

All MAC Address interface

Factory Default

To reset the switch to the default configuration. Click Default to reset the configuration to the default values.



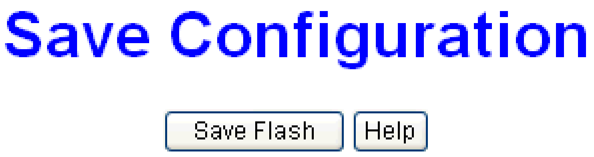
Please click **[Default]** button to restore factory default setting.

□ Keep current IP address setting
□ Keep current username & password

Factory Default interface

Save Configuration

To save a configuration that you have created in the system, click Save Flash to save the configuration to the flash memory.

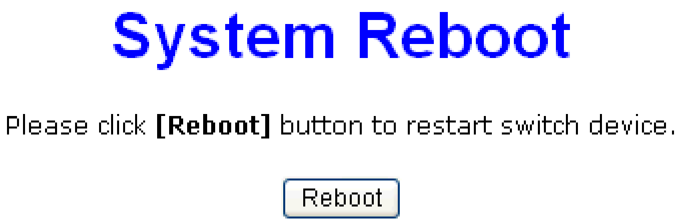


Save Configuration

Save Configuration interface

System Reboot

To reboot the switch in software, click Reboot to reboot the system.



System Reboot

Please click **[Reboot]** button to restart switch device.

System Reboot interface

Troubleshooting

- Verify that you are using the right power cord/adapter (DC 24-48V), do not use a power adapter with a DC output greater than 48V, or it will damage the switch.
- Select the proper UTP cable to construct the user network. Correct cable types are: unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Use Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnostic LED Indicators:** the Switch can be easily monitored through the panel

indicators to assist in identifying problems, which describes common problems that the user may encounter.

- If the power indicator does not turn on when power is applied, there may be a problem with the power supply. Check for loose power connections, power losses or surges at the power supply. If the user cannot resolve the problem, contact the local dealer for assistance.
- If the Industrial switch LED indicators are normal and the connected cables are correct but the packets still cannot transmit, check the system's Ethernet devices' configuration or status.

Technical Specifications

The 8 10/100TX plus 2 100FX managed industrial switch technical specification is the following.

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX and 100Base-FX Fast Ethernet IEEE802.3x Flow Control and Back-pressure IEEE802.1d spanning tree / IEEE802.1w rapid spanning tree IEEE802.1p class of service IEEE802.1Q VLAN Tag
Protocol	CSMA/CD
Management	SNMP management Web interface management One RESET button to return to the system default settings
RFC Standard	RFC2030 SNTP RFC 2821 SMTP RFC 1215 Trap RFC2233 MIBII RFC 1157 SNMP MIB RFC 1493 Bridge MIB RFC 2674 VLAN MIB RFC 2665 Ethernet like MIB RFC 2819 RMON MIB Private MIB

SNMP Trap	Up to 3 Trap stations Cold start Port link Up Port link down Authentication Failure Private Trap for power status Port Alarm configuration Fault alarm, X-Ring Redundancy change
Technology	Store and forward switching architecture
Transfer Rate	14,880 pps for 10Base-T Ethernet port 148,800 pps for 100Base-TX/FX Fast Ethernet port 1,488,000 pps for Gigabit Fiber Ethernet port
Transfer packet size	64 bytes to 1522 bytes (with VLAN tag)
Packet filter	4 types of packet filter rules with different packet combinations: ■ All of packet ■ Broadcast/ multicast/ flooded unicast packet ■ Broadcast/ multicast packet ■ Broadcast packet only
MAC address	8K MAC address table
Memory Buffer	1Mbits
LED	**Per port:** Link/Activity (Green), Full duplex/Collision (Orange) **Per unit:** Power (Green), Power 1 (Green), Power 2 (Green), Fault (Orange), Master (Green)

Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5 cable EIA/TIA-568 100-ohm (100m)
Optical cable	■ **SC (Multi-mode):** 50/125um or 62.5/125um ■ **SC (Single mode):** 9/125um or 10/125um ■ **Available distance:** 2KM (Multi-mode) / 30KM (single-mode) ■ **Wavelength:** 1310nm (multi-mode/ single mode)
Back-plane	5.6Gbps
Packet throughput ability	8.3Mpps at 64bytes
Power Supply	24 ~48 VDC Redundant power with polarity reverse protection function and removable terminal block for master and slave power.
Power consumption	7.5 Watts
X-Ring	2 ports for X-Ring to provide redundant backup feature and the recovery time below 300ms. The ring ports can be defined by the Web interface.
VLAN	Port based VLAN IEEE802.1Q Tag VLAN. Both of port based and Tag based VLAN group up to 256 VLANs.

Class of service	IEEE802.1p class of service 4 priority queues per port.
Quality of service	Port based/Tag based, IPv4 Tos, IPv6 Different Service.
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.
IGMP	IGMP v1, v2 and Query mode Up to 256 multicast groups.
SMTP	Simple mail transfer protocol.
SNTP	Simple Network time protocol.
Management IP security	IP address security to prevent unauthorized intruder
Port mirror	TX packet only RX packet only, Both of TX and RX packet
Firmware update	TFTP firmware update TFTP backup and restore
Alarm	One relay output for port breakdown and power fail alarm Normally Open contact Alarm Relay current carry ability: 1A @ DC24V

Bandwidth control	■ Ingress packets filter and egress packet limit. ■ The egress rate control supports all packet types and the limit rate range is from 100 kbps to 102400 kbps or to 256000 kbps for gigabit ports, and zero means no limit. ■ Ingress filter packet type combination rule for Broadcast/Multicast/Flooded Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. ■ The ingress packet filter rate range is from 100 kbps to 102400 kbps or to 256000 kbps for gigabit ports, and zero means no limit.
DHCP client	DHCP client function to obtain IP address from DHCP server
Install	DIN rail kit and wall mount (optional)
Operation Temp.	-10℃ to 70℃
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40℃ to 85℃
Case Dimension	IP-30, 72 mm (W) x 105 mm (D) x 152mm (H)
EMI	FCC Class A CE EN6100-4-2 CE EN6100-4-3 CE EN-6100-4-4 CE EN6100-4-5 CE EN6100-4-6

Safety	UL cUL CE/EN60950
Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)